Towards a National Security Analysis Approach via Machine Learning and Social Media Analytics

PEDRO CARDENAS-CANTO

Towards a National Security Analysis Approach via Machine Learning and Social Media Analytics

Pedro Cárdenas Canto

A Thesis presented for the degree of
Doctor of Philosophy at Durham University

Department of Computer Science
Durham University
United Kingdom

December, 2022

Towards a National Security Analysis Approach via Machine Learning and Social Media Analytics

Pedro Cárdenas Canto

Submitted for the degree of Doctor of Philosophy
December 2022

Abstract

Various severe threats at national and international level, such as health crises, radicalisation, or organised crime, have the potential of unbalancing a nation's stability. Such threats impact directly on elements linked to people's security, known in the literature as human security components. Protecting the citizens from such risks is the primary objective of the various organisations that have as their main objective the protection of the legitimacy, stability and security of the state.

Given the importance of maintaining security and stability, governments across the globe have been developing a variety of strategies to diminish or negate the devastating effects of the aforementioned threats. Technological progress plays a pivotal role in the evolution of these strategies. Most recently, artificial intelligence has enabled the examination of large volumes of data and the creation of bespoke analytical tools that are able to perform complex tasks towards the analysis of multiple scenarios, tasks that would usually require significant amounts of human resources.

Several research projects have already proposed and studied the use of artificial intelligence to analyse crucial problems that impact national security components, such as violence or ideology. However, the focus of all this prior research was examining isolated components. However, understanding national security issues requires studying and analysing a multitude of closely interrelated elements and constructing a holistic view of the problem.

The work documented in this thesis aims at filling this gap. Its main contribution is the creation of a complete pipeline for constructing a big picture that helps understand national security problems. The proposed pipeline covers different stages and begins with the analysis of the unfolding event, which produces timely detection points that indicate that society might head toward a disruptive situation. Then, a further examination based on machine learning techniques enables the interpretation of an already confirmed crisis in terms of high-level national security concepts.

Apart from using widely accepted national security theoretical constructions developed over years of social and political research, the second pillar of the approach is the modern computational paradigms, especially machine learning and its applications in natural language processing.

Declaration

The work in this thesis is based on research carried out at the Department of Computer Science, Durham University, United Kingdom. No part of this thesis has been submitted elsewhere for any other degree or qualification and it is all my own work unless referenced to the contrary in the text.

Acknowledgements

I am grateful to my mentors, Professors Georgios K. Theodoropoulos, Ioannis Ivrissimtzis and Boguslaw Obara for their guidance throughout my PhD.

I want to thank to the Consejo Nacional de Ciencia y Tecnología (CONACyT) for funding this research.

Last but definitely not least, I would like to thank my wife and children (Dulce, Alejandro and Ximena) for their tremendous support within every second of this journey.

Contents

List of Figures

List of Tables

List of Algorithms

Chapter 1

Introduction

In many aspects, the information revolution has been a catalyst for rapid changes that are transforming modern societies. New technologies, acting as a loudspeaker, amplify discussions of political and social affairs in front of a worldwide audience, and set the agenda of the most strategic topics of interest. Social movements, and various other actors, take advantage of the available digital tools to disseminate information at an unprecedented scale, with often unpredictable ramifications that can be either positive or negative.

On the one hand, positive social traits, such as democratic deliberation, parrhesia[1] or even orderly social protests, can be facilitated. On the other hand, we have the negative aspects, including propaganda of subversive groups, unsubstantiated speculation, or deliberate disinformation aiming at creating fear amid the population. These would often lead into disruptive situations, potentially evolve into instability episodes and eventually, in some cases, affect the very integrity of a state.

Social networking services as Twitter and Instagram can take simple text, image or video messages and turn them into a viral phenomenon. key characteristics of such a mechanism is a certain degree of parrhesia [2], which opinion leaders can convert it into beliefs, sometimes leveraged by social anomie[2]. These types of phenomena are usually unfolding in an environment characterised by a lack of individual confidence,

[1] According to [1], parrhesia refers to the frank of speech.

[2] Improper expressions with irregular words such as insults or offensive expressions [3].

and the absence of social rules, as well as absence of the institutions of governance [3].

National Security is a complex social and political sciences term, examining those factors that tend to undermine the stability of a nation, also called *vulnerabilities*, or *endangered elements*. In national policy terms, and depending on the specific nation's interests, the identified vulnerabilities would usually cover a broad spectrum of events and activities, including, for example, natural disasters, man-made accidents, terrorism and espionage. Due to the complexity and the ever changing nature of real-world events, the development of a national security policy and, therefore, governance, has to deal with significant methodological challenges. On the one hand, threats vary from country to country [4–6], and on the other, new types global threats are emerging, which need to be dealt to maintain the sought after national stability [5].

The risks/threats mentioned before can be analysed from multiple viewpoints, through a variety of approaches. In a widely used framework, outlined in the United Nations Development Program [7], seven elements, also called Human Security components, describe the most common ways national security can be destabilised: health security (linked to being free from disease or infection); food security (complete access to food); economic security (linked to an assured basic income); personal security (being protected from violence and other forms of threats); political security (protection of fundamental human rights and freedoms); communal security (security of cultural identities) and environmental security (access to sanitary water supplies and other basic needs such as clean air).

Keeping the internal balance amongst these seven human security components mentioned above, is a challenging national security task. From the increasingly common now days street riots, to the unprecedented in our lifetime effects of the recent pandemic, the adverse effects of an event can be observed in than one human security component, in a variety of domains: health care, public order, environment, employment, water, food, etc. (see Figure 1.1). Consistent with this observation is the behaviour of the Global Peace Index [8], with the anti-government displays increasing by 244% around the world from 2011 to 2019. These figures suggest that national security components are becoming increasingly interconnected, and

are sensitive to a multitude of different situations.

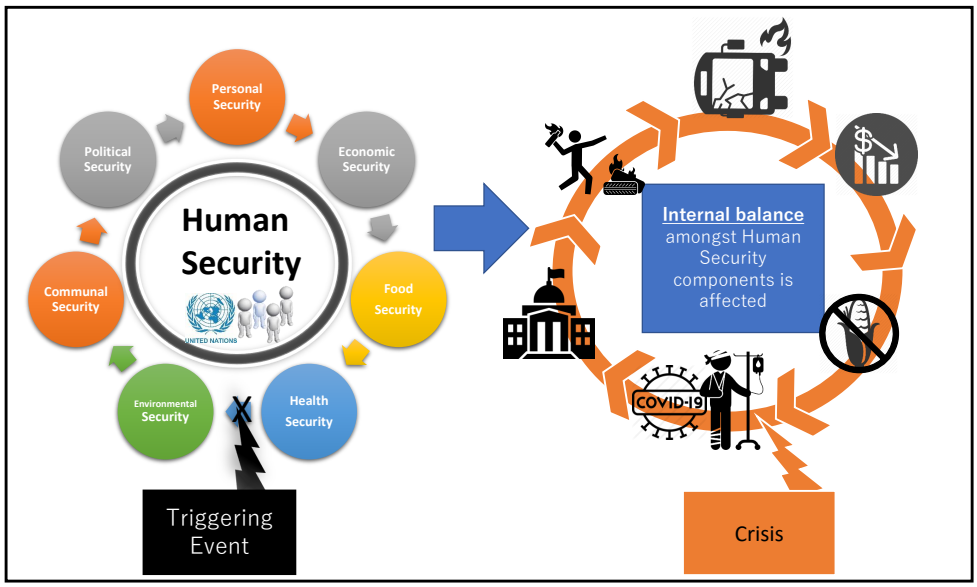


Figure 1.1: Human Security Components. The figure illustrates how once a triggering event starts unfolding, multiple human security components can be affected. As the crisis evolves, the number of affected components increases, creating instability scenarios that undermine national security.

Figure 1.1 illustrates the interconnection between national security components. Once a triggering event has affected a human security element, other components can be successively stricken as the crisis escalates, or even at the aftermath of it. The COVID-19 pandemic gives a very characteristic example of this phenomenon. At the beginning, it was the health that was severely disturbed. As the crisis unfolded, in a knock-on effect, multiple other components were progressively contaminated, such as economic security, food security, and personal security, creating instability at levels that posed serious challenges to national security [12].

1.1 Linking National Security and Human Security

The term national security has been evolving at the same rate as the world is changing, since a concept adopted ten years ago has rapidly changed a decade later. This fact reflects the importance of keeping updated on those aspects that directly impact a state's security. A key fact to understand such an effect is to study the relationship between national security and human security.

As described in [15], the main objective of national security is the defence of territorial integrity and sovereignty from an external incident. By contrast, the importance of human security lies in centring on the welfare of people, which is branched into seven domains [7]: food security, economic security, health security, environmental security, community security, personal security and political security.

Threats such as a pandemic, biological warfare or cyberterrorism, which uses more sophisticated means [4], can create a significant imbalance amongst human security components. Therefore, protecting people from the ravages of the alterations of human security elements, such as lack of food, water or massive contagion of diseases, represents a significant task since it strengthens the legitimacy, stability, and security of a state [16]. By contrast, national security has a different scope which is focused on contributing to maintaining the development of a country [17]. In connection with both contexts, state security and human security are mutually supportive, which is why the view proposed by the United Nations [7] points out that seven human security elements enable the detection and examination of those vulnerabilities that might affect the stability of a nation. In addition, and to reinforce such a view, [17] described that without security, there is no development of a state, and vice versa; without development state's security will be altered (see Figure 1.1).

1.2 Data Analytics and Big Data in the Context of National Security

Since ancient times, information has represented a critical asset that influences decisions, and during the last decade, information volumes have increased to such an extent that numerous techniques are required to explore and therefore extract valuable insights that contribute to the decision-making process. The examination of vast volumes of data (Big Data), also called data analytics [18], enables identifying significant aspects to solve a wide range of problems.

In the era of Social Media and Information Technologies, data has a myriad of nuances as Internet users post messages, pictures and files, in such a way that an idea can be conveyed in a muti-flavoured way. Then, the big challenge lies in dissecting the information and unveil hidden patterns within the data.

Countries around the world are concerned about handling data since it represents sensitive information, but in the context of maintaining the stability of a state, the way in which data is processed creates a dilemma because, on the one hand, some nations consider that technologies such as machine learning can process sensitive data without human supervision, on the other hand, some countries contemplate human-involvement is essential to decide over the way to collect and process such information.

Irrespective of the posture, the interest in examining data through artificial intelligence has rapidly grown in areas such as defence or policymaking [19]. Governments worldwide have released ambitious programmes [19] in order to lead such a field to address threats to national security [20].

As a result, there has been an intense fusion between artificial intelligence, defence and intelligence concepts [19, 21] to create a broad range of tools to pinpoint pernicious threats that tend to destabilise the fragile balance amongst those components that are linked to the stability of a state. Detecting patterns, identifying anomalies or providing valuable insights that improve situational awareness and decision-making are some of the avenues to contribute to the aspects mentioned above. However, categorising these tasks according to the type of problems

they solve can facilitate the dissection and, therefore, the examination of national-security-related issues.

The categorisation proposed by [22] and depicted in Figure 1.2 provides an examination of artificial intelligence and national security based on three main processes: Organisational Process Automation, Cyber Security, and Augmented Intelligence Analysis. The former procedure (Organisational Process Automation) clusters those tasks linked to automate organisational, administrative and data management processes. The second process (Cyber Security) is focused on spotting abnormal network traffic or malicious software and provide information to create a timely response to anomalous behaviour. The third operation (Augmented Intelligence Analysis) derives insights from unstructured data to improve the intelligence process workflow by lowering the volume of content that is subject to human assessment.

In consonance with the Augmented Intelligence Analysis process, the Cognitive Automation sub-process focuses on replicating the human sensory procedure to reduce the time required for human operators to interpret large volumes of data, such as speech-to-text transcription, machine translation, video summarisation or object classification.

The core of the Filtering, Flagging and Triage sub-process lies in analysing bulk data using automated volume reduction systems to filter, query and select material for examination by incorporating artificial intelligence to spot more connections and correlations within data more efficiently than human operators.

The Behavioural Analytics sub-process relies on deriving insights and generating forecasts about human behaviour in order to detect potential threats that might affect public life. Moreover, and following the motivation described in Section 1.4, this thesis is aligned to the Behavioural Analytics subprocess. Since the Alert Mechanism described in Chapter 3 generates the detection of tipping points of an incident, and the subsequent Chapters (4 to 6) detail different behavioural insights such as radical behaviour, ideology and web insights which can be extracted to create a big picture to enable the interpretation of the disruptive situation.

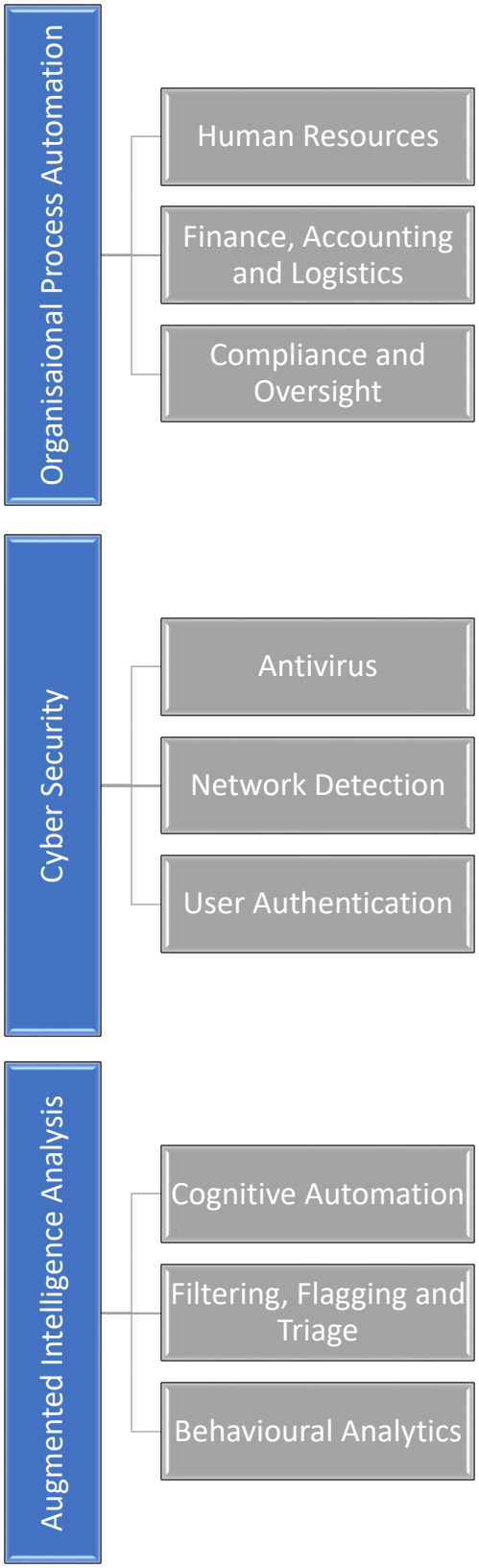


Figure 1.2: National Security uses of Artificial Intelligence. Adapted from [22].

1.3 Gap analysis on the use of machine learning to analyse new national security threats and challenges

This section describes the current gap regarding the usage of machine learning techniques to cope with national security problems. As described previously, the study of national security represents a core task because the internal stability of a state is a fragile environment that can be disrupted due to the sudden unbalance of human security components.

However, the examination of such an imbalance requires complex processes that link two fields. On the one hand, national security theories and, on the other hand, machine learning techniques. This complex symbiosis of elements enables the study and dissection of critical edges involved in maintaining the state's stability and detecting threats that tend to affect people's security.

Creating the national-security-technology bonding implies the analysis of multiple and intricate aspects, which in connection to the categorisation described in [22], outlines the complexity to analyse such an essential issue.

Different efforts have been proposed to study national-security-related aspects using the Behavioural Analytics view explained in [22] (see Table 1.1). All these efforts have used different avenues, such as examining radical behaviour or ideology. Yet thus far, the previous endeavours have been focused on addressing such aspects separately. Nonetheless, to the best of my knowledge, no methodology has been centred on gathering the study of multiple aspects/threats, enabling in such a way the timely detection of tipping points and, then, the extraction of dissimilar behavioural insights (web insights, radical behaviour and ideology) that contribute to the creation of a holistic view of an incident.

Table 1.1: Related Works aimed at analysing National Security using Artificial Intelligence

Related Work	Description	Analysed Threat
Community Policing and the Prevention of Radicalisation (CoPPRa) [23].	Project financed by the European Union and co-funded by the Belgian Federal Police, aims to enhance the capacity of first-line police officers to prevent radicalisation.	Radicalisation
Semantic Analysis against Foreign Fighters Recruitment Online Network (SAFFRON) [24].	A system centered on detecting early detection of foreign fighters' recruitment by terrorist groups in Europe, focusing on ISIS and Al-Qaeda.	
Detecting and Analysing Terrorist-related online contents and financing activities (DANTE) [25].	The project is focused on detecting terrorist financing activity.	
Partnership against violent radicalisation in the cities (PRACTICES) [26].	The project is centred on examining violent radicalisation in European cities.	
Terrorism pReventIon Via rAdicaLisation countEr-NarraTive (TRIVALENT) [27].	The project is focused on understanding the root causes of violent radicalisation	
Early Model Based Event Recognition using Surrogates (EMBERS) [28–30].	The system was designed to forecast significant societal events.	Radicalisation (Civil unrest incidents)

1.3.1 Radicalisation

As described in [31], the term radicalisation has been extensively studied, and it refers to the process through which an individual comes to support or be involved in extremist ideologies. However, according to the Organisation for Security and Co-operation in Europe [31], such a process does not necessarily reflect a threat to society as long as it is not linked to violence or other types of behaviour that tend to alter the internal stability of a state.

As part of these alterations to security, terrorism constitutes a critical aspect since there have been numerous incidents worldwide where sophisticated methods were used to spread radical ideologies and recruit people [32]. From a national security perspective, terrorism constitutes a common threat that has been included in different security programmes around the world [15, 22], and they consider it a severe emergency because it can affect the internal components that maintain stability within the state.

Due to the importance of radical activities and their impact on national security, different efforts have been proposed to address different tasks, such as violent activity or unrest incidents, using artificial intelligence methods.

In line with this aspect, radicalisation diagnostic tools such as CoPPRa [23] provides an explanation of such an issue and its factors, followed by indicators focused on identity (changing names, clothing, physical appearance), ideology (contact with extremist groups, propaganda, secret meeting) and behaviour (travel patterns or radical demonstrations).

One more approach is DANTE [25], which offers data mining and analytics analysis aimed at detecting, retrieving, and analysing online terrorist-related content from the Surface and Deep Web, including Dark Nets.

The EMBERS project [28, 29] is a large-scale big-data analytics system aimed at forecasting societal events, such as civil unrest incidents and disease outbreaks, using publicly available data.

1.3.2 Societal Event Forecasting

Societal events such as civil unrest or riots could significantly impact the fragile balance that exists between the features that integrate the human security components (see Figure 1.1): political security, personal security, economic security, food security, health security, environmental security and communal security.

Forecasting such types of incidents provides crucial information that contributes to timely decision-making and resource allocation [33]. Moreover, the importance of such aspects lies in the fact that two main factors have leveraged and accelerated the event prediction process: Firstly, the development of complex computational algorithms (machine learning and deep learning), and secondly, the accessibility of massive data, such as social media, blogs, news, etc. As a result, various approaches that use deep learning have been proposed to predict incidents, as shown in Table 1.2.

Table 1.2: Related work to Deep Learning studies aimed at analysing civil unrest events.

Method	**Dataset**	**Type of task**	**Reference**
LSTM	GDELT	Regression	[34]
LSTM	ICEWS, GDELT	Regression	[35]
CA-LSTM	GDELT	Regression	[36]
GRU	GDELT	Binary Classification	[37]
DynamicGCN	ICEWS, News reports	Binary Classification	[38]
Cov-LSTM	IARPA, GSR, Blogs, Google Trends	Classification	[39]
Glean	ICEWS, News reports	Classification	[40]

1.3.3 Recurrent Neural Networks for predicting Civil Unrest events

Historical statistics of social indicators provide information about societal behaviour over time. Due to the time sequence of events, predicting these types of episodes requires computational models that can capture and predict how those indicators will move in the future. Civil unrest events fall into this category since their evolution can be studied as time series. Moreover, models such as Long Short-Term Memory (LSTM) [41] or GRU [42] contribute to modelling them.

The idea behind LSTM lies in the fact that it can capture short- and long-term dependencies in time series data, and its efficacy has been tested over traditional methods such as autoregressive models. GRU is another flavour of recurrent neural networks that use fewer training parameters, and consequently, their training consumes less memory leading to a faster training time than other models. The efficacy of this model in addressing civil unrest prediction has been analysed in [37], where the authors considered dissecting the problem into a feature selection process, considering indicators such as social and economic features as their input.

One more effort is the one presented by [39], where an RNN-based model (Cov-LSTM) was proposed. This model uses a combination of convolution layers and LSTM layers to predict the incidents. The core of this computational model extracts high-level representations of the event in the form of time series; then, the transformed features are passed to the LSTM model to make the prediction.

A context-aware attention based long short-term memory model (CA-LSTM) is an additional prediction framework proposed by [36] to predict the amount of unrest news of a state. The model used LSTM to learn the hidden representation from the time-series data, then by using a fully connected layer, predict the unrest news amount.

Due to the complexity of analysing societal disturbance events, graphs have shown their effectiveness [38] by encoding structural information to model the relationship between entities and uncover relevant insights into the data [43]. Graph convolutional networks are a variant of Graph neural networks that take advantage

of their structural information. Songgaojun et al. [38] proposed a dynamic graph convolutional network (DyamicGCN) to forecast protests. The research described an encoding method for historical news into a sequence of word graphs.

Finally, [40] proposed a temporal graph learning method aimed at capturing data from historical data, which is based on event knowledge graphs that include two main components: relational and context words. The focus of this research was to predict concurrent events of multiple classes, including civil unrest episodes.

1.4 Motivation and Research Questions

Security and development are two-related concepts that impact each other, and where such a duo constitutes the foundation of national security [17]. Maintaining the internal balance amongst the elements linked to national security, such as the human security components: health security, economic security, food security, political security, personal security, communal security and environmental security, can help support the continuity of the state's development and stability.

Numerous disruptive events around the world [9–11], such as protests, riots, violent episodes or even the COVID-19 pandemic [12, 13], have shown the profound impact of disturbing one or more human security components and, as a result, the affectation of other core elements (see Figure 1.3).

Figure 1.3: Lockdown protests amidst the COVID-19 pandemic in Edinburgh in 2021. Adapted from [14].

Different theoretical approaches to dissecting national security [16, 17], and its components [7] have been used to create policies to identify internal and external threats [4–6]. Moreover, such a view has been complemented by technical efforts aimed at detecting issues such as radicalisation, ideology or violent expressions [23–25, 28]. However, due to the complexity of studying topics linked to security together with the importance of examining in detail the components of national security, a comprehensive methodology that integrates theoretical high-level security concepts

and computational models could contribute to spotting and therefore understanding events that can alter the fragile balance between all human security components. Envisaging the importance of such an aspect, this research project aims to create a new methodology to examine the complex problem centred on analysing those factors that tend to destabilise the internal components that maintain cohesion within a state, namely, national security.

The core motivation to undertake this research is to address the global need to use technology to study, spot and extract core features that enable examining such an essential topic and provide helpful insights that facilitate the decision-making process in the security context. In order to tackle this need, machine learning, together with numerous computational techniques, has been used to create a fine-grained methodology based on two main stages: Warning Period and Crisis Interpretation.

Throughout this work, the endeavour was focused on understanding how the aforementioned computational techniques can be used to answer the following primary research questions:

- **Warning Period**
  - RQ1. Can a Conceptual Framework be designed to examine disruptive events? (addressed in Chapter 2)
  - RQ2. Can an Alert Mechanism be created to detect when people head towards a situation that evokes that both social stability and national security components have been compromised? (addressed in Chapter 3)
- **Crisis Interpretation**
  - RQ3. Can the analysis of virtual communication channels disclose that national security has been affected? (addressed in Chapter 4)
  - RQ4. Can radical behavioural traits be detected during a disruptive incident? (addressed in Chapter 5)
  - RQ5. Can ideological traits be detected during a disruptive incident? (addressed in Chapter 6)

1.5 Thesis Contributions

This thesis presents contributions to the state-of-the-art in the following areas:

- The design of a conceptual framework centred on analysing disruptive events by the use of supervised and unsupervised learning (Chapter 2).
- The development of an Alert Mechanism via a deep learning network and supervised learning methods. The mechanism is focused on spotting points (tipping points) that reflect that the society may be heading towards a situation where a disruptive event may unbalance those elements (human security components) that tend to keep the stability of the state (Chapter 3).
- The creation of a new methodology to analyse virtual communication channels based on hybrid warfare concepts to detect national security instabilities along with expressions of violence. The analysis of such web resources is supported via supervised learning methods, data analytics, and natural language processing techniques (Chapter 4).
- The creation of a methodology to identify radical behavioural traits using natural language processing techniques, data analytics, and unsupervised learning (Chapter 5).
- The creation of a methodology to spot ideological traits (authoritarianism and hostility), using unsupervised learning, natural language processing techniques and data analytics (Chapter 6).
- The evaluation of the methodologies described previously, using incidents with dissimilar nature and nuance such as protests and a health crisis (COVID-19), see Chapters 2-7.

1.6 Publications

At the the time of submission, six Chapters of this thesis had been submitted for publication or published in conferences.

- **Cárdenas P.**, Theodoropoulos G., Obara B. and Kureshi I.: A Conceptual Framework for Social Movements Analytics for National Security. The International Conference on Computational Science, (2018) **(Chapter 2)**.

- **Cárdenas P.**, Theodoropoulos G., Obara B. and Kureshi I.: Defining an alert mechanism for detecting likely threats to National Security. IEEE International Conference on Big Data. USA, (2018) **(Chapter 3)**.

- **Cárdenas P.**, Theodoropoulos G. and Obara B.: Web Insights for National Security: Analysing Participative Online Activity to Interpret Crises, IEEE International Conference on Cognitive Informatics and Cognitive Computing, Italy (2019) **(Chapter 4)**.

- **Cárdenas P.**, Theodoropoulos G. and Obara B. and I. Kureshi.: Analysing Social Media as a Hybrid Tool to Detect and Interpret likely Radical Behavioural Traits for National Security, IEEE International Conference on Big Data. USA, (2019) **(Chapter 5)**.

- **Cárdenas P.**, Theodoropoulos G., Obara B. and Kureshi I.: Unveiling Ideological Features Through Data Analytics to Construe National Security Instabilities, IEEE International Conference on Big Data. USA, (2020) **(Chapter 6)**.

- **Cárdenas P.**, Theodoropoulos G., Obara B., Ivrissimtzis I. and Kureshi I.: Big Data for National Security in the Era of COVID-19, The International Conference on Computational Science, (2021) **(Chapter 7)**.

- **Cárdenas P.**, Theodoropoulos G., Obara B., Ivrissimtzis I. and Kureshi I.: Big Data for Human Security: The case of COVID-19, Journal of Computational Science, (2022).

These chapters are presented mostly as published, although referencing, and notation has been altered and cross-referencing added for consistency throughout this thesis. The majority of the text is verbatim; however, some stylistic changes have been made for consistency, and some of the text has been extended to explain or discuss certain points in more detail.

Chapter 2

Conceptual Framework

2.1 Introduction

Massive social gatherings and social networks underpinned by technology are two concepts that walk on the same path, especially when the basic structures or essential norms and values of a social system have been disrupted [44]. As a result of a set of social instability issues, a crisis may be triggered and affect the "homeostasis" or internal balance among those elements that maintain the stability of a state such as the economy, public order, health, environment or even life. Social movements are a clear example of these disruptive events because people's behaviour change according to the situation they face, and a violent crowd reaction may lead to an instability scenario.

Microblogging websites and services have served as platforms to express ideas as well as to organise and coordinate crowds during a crisis. Twitter, with over 300 million registered users [45], has seen itself at the centre of several large-scale social movements, with individuals conveying their ideas and frustrations within 280 characters. Hence, understanding the way social movements use microblogs such as Twitter to organise, disseminate ideas, collaborate, coordinate and connect groups or cells of people linked to similar beliefs is, therefore, an essential task to appreciate the evolution of these social events.

There are models that describe how online social movements evolve [46], which parameters describe national security considerations [7, 15], what computational

techniques help to get the private state of individuals, and how to find topics within a data corpus. However, no attention has been paid to create a holistic data analysis framework that links all the above elements and processes it in a timely fashion, to anticipate and detect the core stages of a social movement and when the incident can affect one or more national security variables.

2.2 National Security in the Social Media Era

Security is a complex concept that has different facets depending on the person or entity in question. At times the different types of *security* can be at odds with each other. National security is one of these challenging dimensions. It can be qualified by two main concepts: ensuring the security of the state; and ensuring the security of its people (Human Security) [15]. [7,15] make arguments for how Human Security and State Security are mutually supportive.

Human Security, being people-centred, can be broken down using the United Nations Development Programme [7] into: Economic Security, Food Security, Health Security, Environmental Security, Personal Security, Communal Security and Political Security.

In the digital era, social media tools have been valuable to spread messages related to those major disasters that have struck a society. Hence, social media platforms can help to identify those human security vulnerabilities that have snowballed into a challenge and required immediate attention.

In the light of the Arab Spring revolutions, the Internet in general and social media networks in particular have gained attention as essential instruments for organising people and communicating ideas and plans. This make social media the catalyst that enables movements to mobilise hundreds of thousands of individuals in a few hours [46, 47]. Social media facilitates the link between social movements and collective action theory, where individuals share common interests or objectives, and they work as a single unit to accomplish their expectations [48].

One of the ways to analyse the evolution of Social Movements which use virtual platforms is described in a circular flow model proposed by Sandoval et.al [46].

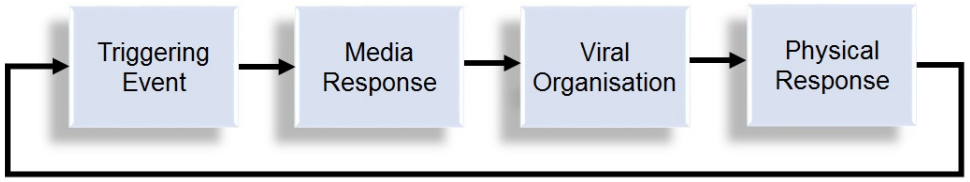


Figure 2.1: Model for Social Media Movements. Adapted from [46].

Figure 2.1 demonstrates the links between the four stages of this model, outlined below.

1. **Triggering Event**: This conceives an opportunity in which individuals tend to become active, as a result of a disruptive incident;

2. **Media Response**: This stage considers that the detonating event brings about an instant response supported by a social media platform which allows people and activists to convey ideas, but at the same time works as a natural channel to uncover important events and show them to a domestic or international audience;

3. **Viral Organisation**: Once a detonating event opens a window for individuals to express their political views using a citizen to citizen channel [2], they create online communities where collective ideas of co-production and collaboration are exchanged to reinforce the community engagement;

4. **Physical Response**: The final stage reflects the power of the massive reaction, where protesters tend to organise resistance using different disruptive actions.

2.3 Conceptual Framework Description (RQ1)

Figure 2.2 outlines an iterative cycle that comprises three main stages, forming the core of our proposed model. These steps allow the dissection of the incident into core elements that interpret the possible evolution of a National Security instability scenario, and at the end, the results can be used to create a fine-grained strategy (Crisis Scorecard) to deal with the event and determine the best course of action.

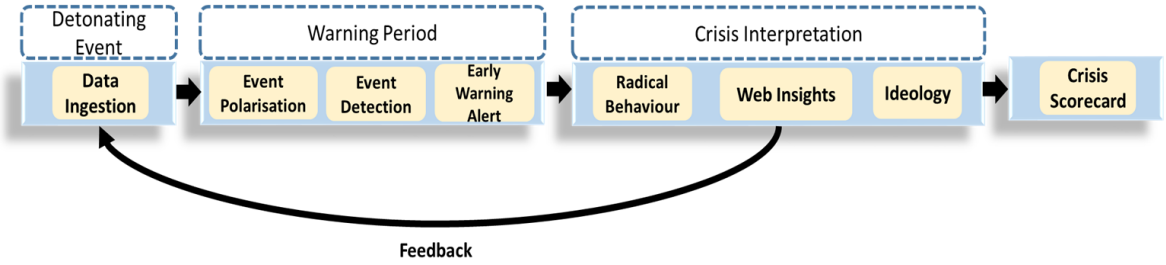


Figure 2.2: Proposed Conceptual Framework to Analyse National Security Aspects.

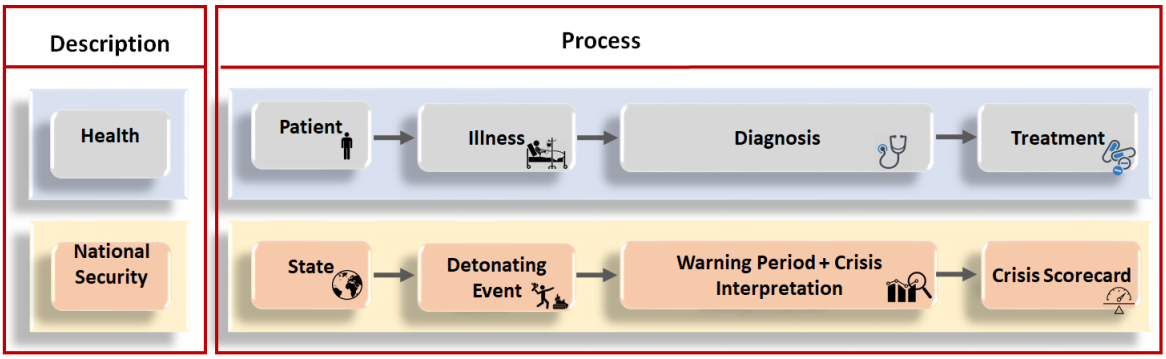


Figure 2.3: Diagnostic Schema example.

This framework takes its root and can be better understood by looking at the medical domain. Within a human health context, diagnosis, detection and interventions are planned using an illness-treatment schema (see Figure 2.3). In line with this idea, the process begins with the patient assessment, and in a national security environment, the state plays the patient role. Therefore the illness can be seen as the crisis event that triggered a crowd reaction (Detonating Event). The Diagnosis involves a twofold process; the first step (Warning Period) detects the "symptoms" such as changes in sentiments or opinions over time. When applying this model to Social media, these symptoms activate a computational analysis to identify which national security variables were affected (Economic Security, Food Security, Health Security, Environmental Security, Personal Security, Communal Security and Political Security).

Once the former analysis reaches a threshold based on domestic national security policies, it starts a second step (Crisis Interpretation) which is focused on recognising and analysing other societal characteristics such as violence; coordination and

cooperation for radical events; emotions and opinions spilt over virtual communities (Web Insights), and a holistic view of the ideas and beliefs involved in the event (Ideology).

These sets of results can avoid "collateral damages" when they are organised in a "Crisis Scorecard" that works as a cluster of support decision indicators that decide the treatment (course of action) that the specialist (decision makers) will prescribe.

When a disruptive event triggers an online crowd reaction, analysing data from virtual platforms provides a rich source of information for understanding its genesis and likely evolution. Hence, examining the steps involved using a holistic approach is an essential point for examining national security instability episodes.

2.4 Framework Component Analysis

2.4.1 Detonating Event

As described in [46], once a political opportunity has triggered a radical societal behaviour, digital information becomes the core asset to identify potential problems.

The preliminary task is to collect those messages or tweets related to the disruptive event; however, as suggested by [46] information flows in four ways: from citizen to citizen, citizen to organisations, organisations to citizens and organisations to organisations. Consequently, selecting the volume of messages that epitomises the disrupting event is the crux of the process.

To tackle this multi-party information exchange process, *retweets* provide a critical conversational infrastructure as they knit all those voices that need to be heard, and those posts are an adopted practice for those users that want to share and spread thoughts, feelings and ideas to new audiences, as well as trying to engage in conversations [49].

2.4.2 Warning Period

A central step that needs to be taken relies on detecting the probable danger that follows the detonating incident. As proposed by [50] a disaster can be distinguished

according to functional time phases. One of these stages is the Warning Period which refers to the length of time where information reveals a likely menace; however, the detection has to be done just before the aftermath of the crisis becomes perceivable.

In a decision-making scenario, the Warning Period represents a core stage due to the outcome that a correct diagnosis may yield, and can contribute to outlining the "course of action" that has to be followed.

National security theory comprises a set of complex societal terms, and computational techniques are a valuable tool to solve a high range of problems. Thus in an attempt to couple both concepts to detect potential significant incidents, a preliminary two-pronged strategy can be evolved, namely Event Polarisation and Event Detection, which are the anteroom of a complex process aimed at spotting when society may be heading towards a point of no return (Early Warning Alert).

Event Polarisation

As social media facilitates the interaction and communication with others [51], people tend to be a primary source of crisis information during a mass emergency event [52], because they use this social software infrastructure to inform their friends, family and acquaintances about their private states (attitudes).

As a result of these set of messages, a significant challenge is to analyse the subjective information to extract and categorise mass opinions that convey a radical idea or oppression feelings [46] and would become the raw material in decision-making.

A computational technique that may be used to detect and analyse Event Polarisation is sentiment analysis. This machine learning technique can be used to classify sentiments into three categories: positive, negative and neutral.

The aim to include this process is not limited to detect opinion polarisations, as sentiment fluctuations symbolise the occurrence of sub-events [53], and it can answer questions that surround a collective negative feeling in a selected geographical region.

Event Detection

A mass emergency event has a large number of individuals and stakeholders sharing information which is why the volume of messages related to a specific topic increases. However, all these disruptive events are not isolated because they include subevents [2] that can represent a significant milestone for an effective intervention.

Upon the Event Polarisation process, the system takes each sentiment stream separately (positive, negative and neutral) and extract the topics related to them. A potential clustering method is Latent Dirichlet Allocation (LDA) as it is one of the most popular techniques for this task and has been used to extract topics in major disasters [54–56].

The next step relies on creating a specialised dictionary that handles words related to human security and is enriched with synonyms to get a reliable wordlist (e.g. ammunition, ammo or munitions).

The fourth step deals with a semantic matching process, where the topics of each cluster is semantically analysed against the wordlist previously created.

Finally, to identify the nature of the event, this component employs the percentage of topics that are related to each Human Security aspect (Economic Security, Food Security, Health Security, Environmental Security, Personal Security, Communal Security and Political Security).

A core aspect is that national security policies are the main reference to evaluate which set of Human Security components describe a local instability scenario.

2.4.3 Crisis Interpretation

A common problem that comes after detecting Human Security issues is to create a "big picture" of the disruptive situation. Figure 2.2 shows in the Crisis Interpretation stage three components focused on 1) analysing digital content to disclose disruptive demeanour (Radical Behaviour), 2) examining virtual communication channels to unveil core features (Web Insights) and 3) construing ideological traits (Ideology).

Radical Behaviour

Violence is a radical expression that can be encouraged using social media tools, and during a massive crisis, extreme groups tend to distribute their ideology through Twitter users [57], generating in such a way mindsets or attitudes towards this type of radical behaviour [58]. In accordance with [58], two behavioural markers that enable to describe the way risk has been increased in the digital platforms are Leakage and Fixation. The former expresses an intent to harm a specific target (facility, person or any other critical objective), whereas the second one refers to the tendency to mention with a higher frequency a critical objective; for this thesis, the term Fixation will consider as critical entities: people, facilities, locations and organisations.

Detecting these radical markers is a computational challenge because it requires the extraction of a wide range of entities such as people, organisations, strategic facilities or even locations along with the interpretation of intentions nuanced by heterogenous actions.

As explained by [59], intentions can be identified using intention verbs which are associated with an intention action (e.g. "I plan to stay at the Theater"); whereas radical intentions comprise a combination of verbs that keep specific semantic properties. In line with this idea, Levin's analysis of verbs [60] provide a strong background to create a radical intention structure which is shown in Table 2.1.

Based on the importance and impact of such aspects from a national security perspective, chapters 5 and 6 will address in detail the dissection of the former radical markers by using natural language processing coupled with other computational techniques.

Table 2.1: Radical Intention Structure using Levin's classification.

Radical Intention Structure	**Example**
[Levin Verb (Desire)] + [Levin Verb (Killing)] + [Entity]	"I want to eliminate wild animals"
[Levin Verb (Desire)] + [Levin Verb (Destroy)] + [Entity]	"I desire to destroy the Police Station"

As suggested by Levin, verbs of **desire** are: want, crave, desire and need; while

verbs of **killing** are: assassinate, eliminate, execute, immolate, kill, liquidate, murder and slaughter and **destroy** verbs are: demolish, destroy, devastate, exterminate and ruin.

Web Insights

When mining tweets, people post URL references related to the event they face, and the frequency of these messages suggest the importance of the content. Therefore crawling the information within those websites may disclose relevant data that enable to comprehend the nature of a crisis (see Figure 2.4).

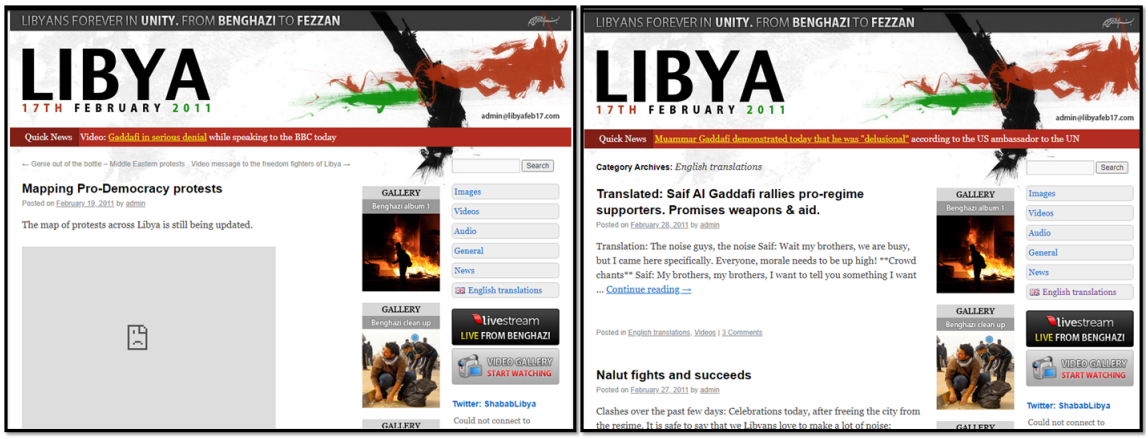


Figure 2.4: Sample of a website created to share information regarding the Libyan conflict in 2011.

The proposed framework requires an iterative loop because the content of these websites needs a complete analysis (Detonating Event, Warning Period and Crisis Interpretation) to identify radical ideology and uncover new events (see Figure 2.2).

Ideology

Tweets allow individuals and organisations to share information that ranges from pictures, videos, weblinks and text. These set of resources can be used to disseminate ideas or beliefs that may influence people's demeanour nuanced by emotional states, namely (anger, disgust, sadness, surprise, fear, trust, joy and anticipation), as described by [63].

The analysis of ideological traits can disclose core aspects that enable to understand the evolution of an incident based on the examination of emotions, an ideological attitude such as authoritarianism and hostility characteristics. At the end of the process, the ideology stage will contribute to creating a holistic procedure to construe the ideological features and radical actions that reign while a disruptive case takes place.

2.5 Analysing the Libyan case

Twitter has been a valuable tool used by activists to "overthrow" established governments. Libya made history when Gaddafi's regime was removed in 2011, and this microblogging service was used to broadcast pictures, telephone numbers, websites and opinions that allowed the escalation of the Libyan uprising.

As a demonstration, this section shows the computational techniques and their results at two sub-stages of the Warning Period: Event Polarisation and the Event Detection (see Figure 2.2) using as input a set of tweets, related to the Libyan conflict using the hashtag #libya, dated from Feb. 1st to Feb. 28th 2011.

As described in Section 2.5.1 only retweets were considered, and from a language analysis standpoint, messages written in English were selected. Consequently, the data corpus were reduced from 28,524 to 20,149 tweets.

2.5.1 Event Polarisation

Before analysing sentiments, the data was cleansed by following three preprocessing steps: 1. URLs, RT and Mention terms were removed; 2. contractions and abbreviations were replaced, and 3. informal ways to convey information (short words) such as: "plz", "pls", "ppl" , "peeps", "pleasert" or "prt" were replaced by its word of origin (e.g. "plz" –> please or "ppl" –> people).

To begin with the Sentiment Analysis process, the Stanford CoreNLP library was used with the Recursive Neural Tensor Network model [61] as our baseline to compute sentiments measures (positive, negative and neutral).

Our data shows that 73% of the analysed messages have a negative polarisa-

tion (see Figure 2.5), which is why these double figures suggest a clear negative orientation.

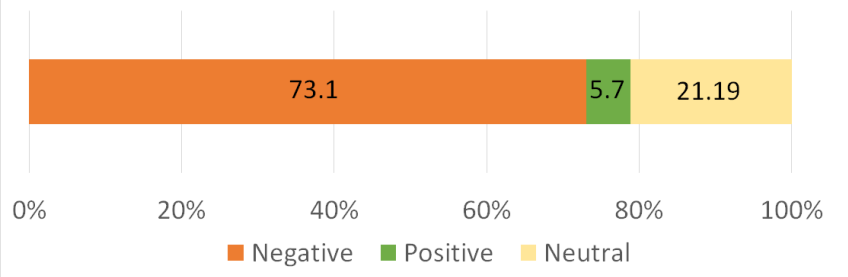


Figure 2.5: Sentiment Orientation

Once the polarisation has been detected, the next step focuses on identifying sentiment fluctuations which can be represented as a positive linear correlation or negative linear correlation. In a similar fashion to [53] we calculated the correlation among the percentage of positive and the percentage of negative messages. A correlation -0.296 suggests that both sentiments were moving towards opposite paths (when positive sentiments tend to decrease, negative sentiments increase), see Figure 2.6). As can be seen in the Figure 2.7 (a), the ThemeRiver visualization [62] shows that the volume of polarised messages (negative, positive and neutral) increased from February 18th to February 25th, and this gives the chance to identify three visible sentiment shifts (A,B and C) and two essential time frames (Feb. 18th to Feb. 21st and Feb. 21st to Feb. 25th).

Figure 2.7(b) shows a timeline of the Libyan conflict, outlining the critical events where the sentiment explosions appeared.

2.5.2 Event Detection

After identifying the sentiment bursts and considering those points as critical subevents, two questions that come to mind are: (1) What topics were conveyed over those time frames? Moreover, (2) are those topics related to national security?

The first question was tackled by using a topic modelling technique known as LDA which was developed by [64]. However, one of the leading issues lies in de-

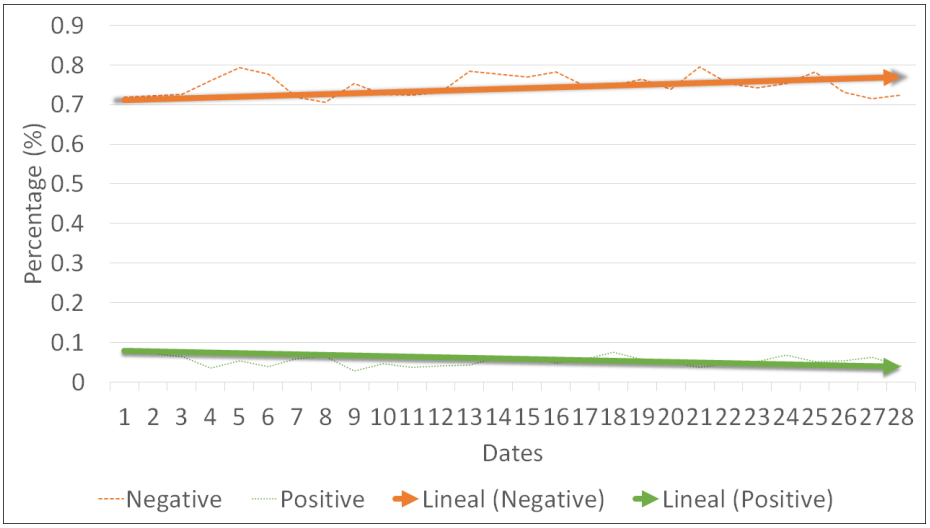


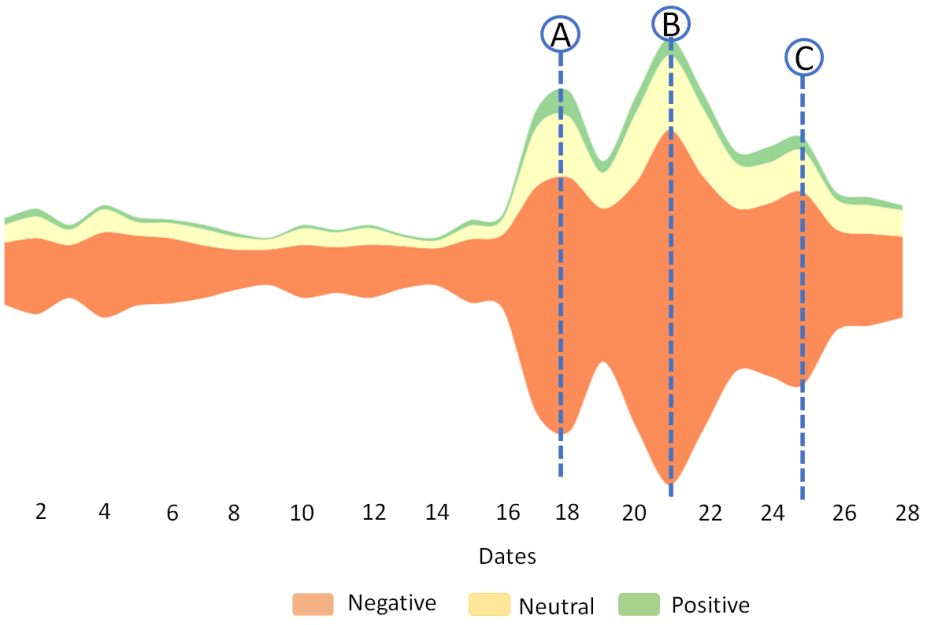
Figure 2.6: Trends on sentiment polarisation during the Libyan incident (February 2011).

termining the number of topics. For this purpose Perplexity analysis was used to evaluate the optimum number of topics, whereas the cross-validation methodology proposed by [65] was used to assess the performance of the topic extraction model.

The second question requires a semantic component to associate those topics that were found in the topic extraction phase, to a Human Security dictionary. One way to deal with this semantic issue was to query the Integrated Public Sector Vocabulary [66], which is a public wordlist that contains a set of terms related to a variety of categories, and some of them are linked to Human Security aspects (Economic Security, Food Security, Health Security, Environmental Security, Personal Security, Communal Security and Political Security). However, to get an enriched dictionary, synonyms were added by using the Wordnet lexical database.

As negative sentiments had a predominant role, the topics extracted from the set of tweets were semantically matched to the expanded dictionary; however, as the volume of tweets had different growth rates, and the number of topics was dissimilar over time, the resulting matched topics were normalised by calculating the percentage of each Human Security aspect per day (see Figure 2.9).

To understand the way Human Security variables behaved over time, a Normalised Cross-Correlation analysis was calculated between all of them; but not only



(a) Sentiment changes

Timeline

February 15: Between 500 and 600 demonstrators protested in front of Benghazi's police headquarters. The protest was broken up violently by police [**].

February 16: About 200 demonstrators protesting the arrest of a human activist take to the streets in the coastal city of Benghazi [*].

A. February 18: In Benghazi, human rights groups and *protesters claim they are under attack* by pro-government forces [*].

B. February 21: In Benghazi, *protesters took control of the streets, looting weapons* from the main security headquarters [**].

C. *February 25: Thousands took to the streets of Tripoli to protest with the civilian death toll rising [**].*

U.S. President Barack Obama signs an executive order freezing Moammar Gadhafi's assets [*].

Sources: * CNN (2011) A timeline of the conflict in Libya. Available at: http://edition.cnn.com/2011/WORLD/africa/08/18/libya.timeline/index.html (Accesed: 22 November 2017).

** Global News (2011) Timeline: Libyan civil war (February 15 – October 20, 2011). Available at: https://globalnews.ca/news/168180/timeline-libyan-civil-war-february-15-october-20-2011/ (Accesed: 22 October 2020)

(b) Timeline of Events

Figure 2.7: Sentiment Fluctuations and Timeline of Events in Libya (February 2011).

in those time frames where the sentiments burst, but a "step before" because it is essential to understand what happened in those previous days. Hence, the Breakout anomaly detection algorithm released by Twitter was used to identify those previous variation points suitably.

As Figure 2.8 shows, the Breakout algorithm detected two time frames before the changes in sentiment; however, the area shaded in red (AA) and the one shaded in blue (BB and CC) were analysed to understand what happened before and during the sentiment fluctuations appearance.

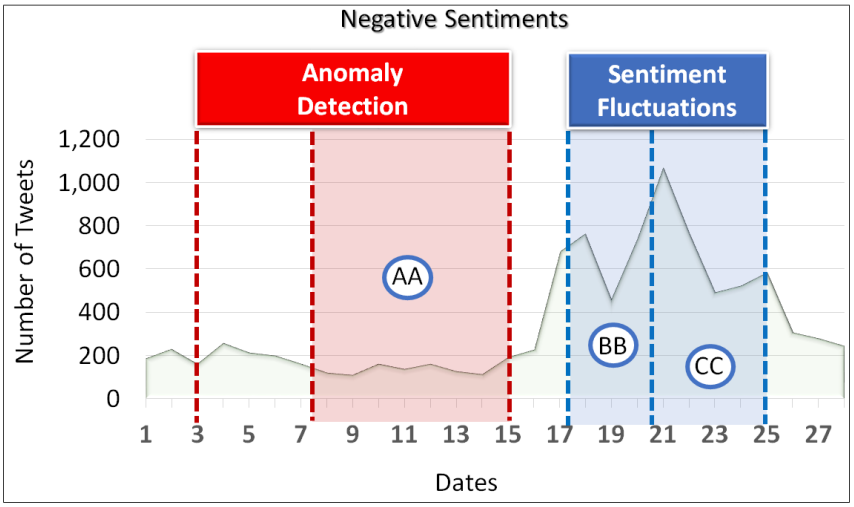
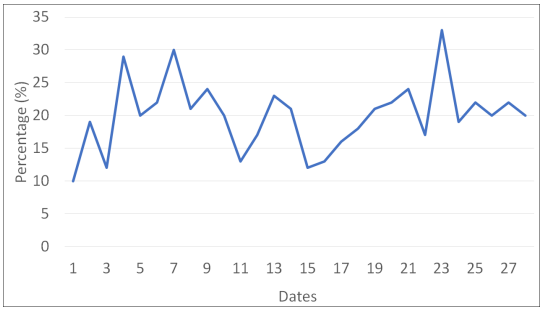
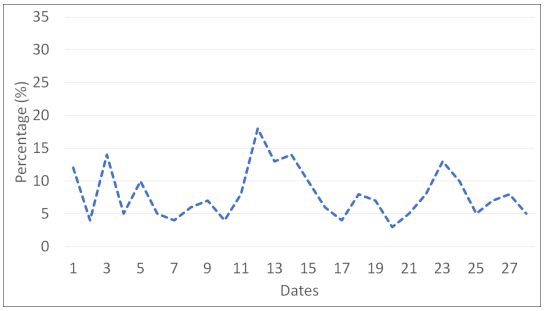


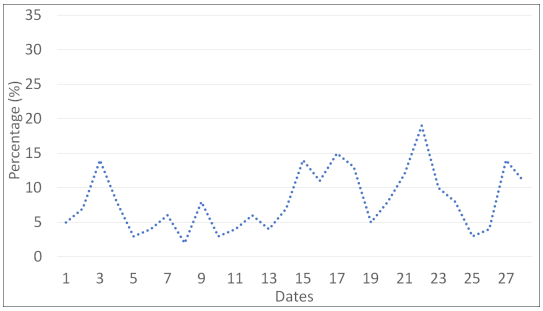
Figure 2.8: Sentiment Fluctuations and Breakout Detection during the Libyan conflict (February 2011).



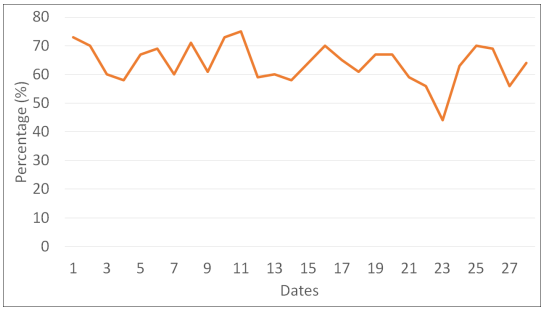
(a) Percentage of terms related to Health Security



(b) Percentage of terms related to Personal Security



(c) Percentage of terms related to Food Security



(d) Percentage of terms non-related to Human Security aspects

Figure 2.9: Percentages of Human Security components during the Libyan incident (February 2011)

Topics	Correlations			Percentage Difference (%)	
	Anomaly Detection	Sentiment Fluctuations			
	(AA)	(BB)	(CC)	(AA) to (BB)	(BB) to (CC)
	Feb. 9 - Feb. 16	Day 18 - Day 21	Day 21 - Day 25		
Public Order -Defence	0.2132	0.3133	0.503	46.95%	**60.55%**
Public Order -Life	0.3109	-0.3919	0.4897	-226.05%	**224.96%**
Public Order - Information	-0.53079	0.08	0.2473	115.07%	**209.13%**
People - Defence	-0.6181	0.7065	-0.5028	214.30%	-171.17%
People - Health	-0.3129	-0.7065	0.6383	-125.79%	**190.35%**
People - Life	-0.1256	-0.2175	0.8116	-73.16%	**473.15%**
Information - Government	0.525	0.3002	0.7492	-42.82%	**149.57%**
Information - Defence	-0.3551	-0.3248	0.8323	8.53%	**356.25%**

Table 2.2: Correlation of Human Security Parameters

Table 2.2 illustrates the cross-correlation results between some of the Human Security aspects such as Public Order, People and Information, and it outlines the following relationships: Public Order – Defence, Public Order – Life, Public Order – Information, People – Defence, People – Health, People – Life, Information – Government and Information – Defence.

According to the Table 2.2 two scenarios can be identified. The first one (AA to BB) shows that only four out of eight variables had positive increments. On the other hand, the second scenario (BB to CC) shows in as many as seven out of eight analysed variables had positive increases. Hence, the latest scheme suggests that people were strongly engaged in topics related to Public Order and Life (224.96%), Public Order and Information (209.13%) and People and Life (473.15%).

As a result, the more positive increments that have been found over a time frame, the more attention that has to be paid to them. This is a key feature that triggers the next stages (Alert Mechanism and Crisis Interpretation). However, the nature of the event and National Security policies will decide which set of Human Security aspects have to be considered to create the Crisis Scorecard and the suitable percentages that have to be reached to activate the following phases.

2.6 Conclusion

In this chapter, we proposed a holistic conceptual framework that utilises computational techniques for examining Social Movements and detecting threats to Human Security.

To demonstrate the feasibility of the framework, we presented a preliminary analysis of tweets related to the Libyan events focussing in particular on the Warning Period. This analysis has helped to identify two essential frames where critical events occurred. Another core result was the detection of those Human Security variables that had positive variations. This suggests that the more positive increments, the more attention that has to be paid to them because these set of changes showed which aspects epitomised the social disruption.

This preliminary experimental phase has already pointed to some challenges

with regard to the components involved in the Warning Period phase. First, slang expressions are still a great challenge because the language has semantic variations from country to country. Hence, creating a robust dictionary may improve radical behaviour detection. Second, spelling mistakes correction is an important issue that Natural Language Processing (NLP) has to deal with because it can improve the Event Detection Phase. Third, microblogging platforms tend to spread opinions, but anonymity within this virtual communities is hard to probe.

Chapter 3

Defining an Alert Mechanism for Detecting likely threats to National Security

3.1 Introduction

Social Media as a means of communication, has changed the way society interacts because individuals can convey messages, pictures and videos to a worldwide audience. When a society faces instability issues, information shared tends to pertain to those aspects that have affected the internal balance of the state such as health, public order, life, environment or economy [7].

As a result of this state of insecurity, the affected communities engender support towards a groupthink, and this group of beliefs can reach an audience of critical mass that may lead to a disruptive and chaotic scenario.

In line with this idea, in Chapter 2 a conceptual framework for social movements analytics that might threat national security stability was presented focusing on three interconnected stages, namely, Detonating Event, Warning Period and Crisis Interpretation (see Figure 3.1).

The former stage called the Detonating Event relies on collecting those messages that epitomise a disruptive incident.

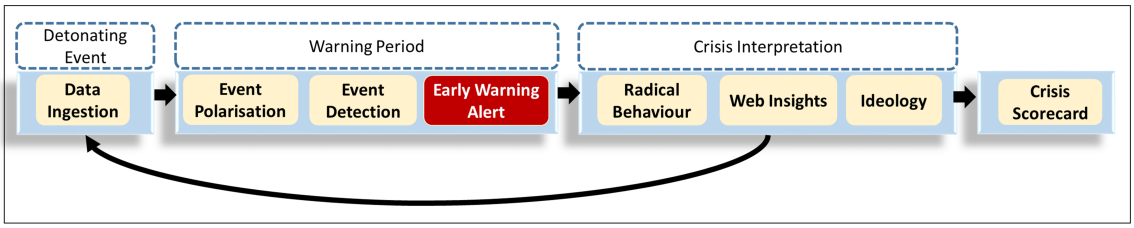


Figure 3.1: The proposed Conceptual Framework for Social Movements Analytics, described in [67].

The second stage (Warning Period), analyses the probable danger that follows the detonating incident by considering two essential features; the first one is the examination of opinion polarisations and the detection of the occurrence of subevents, and the second one evaluates which national security components describe the local instability scenario.

The third stage (Crisis Interpretation), comprises a set of complex computational techniques to construe the crisis by creating a holistic picture of it, which runs from radical behavioural elements to the analysis of the involved stakeholders.

This chapter focuses on the "Warning Period" phase of the proposed framework. A mechanism is presented to decide whether a detected incident represents a likely threat to National Security, and based on this assumption determine whether the situation is heading towards a major disruption.

The Alert Mechanism can identify points where society may be heading towards a situation where a major disruption may affect the "homeostasis" or internal balance amongst those components that keep the stability of the state (i.e. a tipping point).

3.2 Towards an Alert Mechanism (RQ2)

A crisis event can be understood as a critical situation where large-scale events can affect a community or a country where national security features are also affected, namely Human Security aspects (Economic Security, Food Security, Health Security, Environmental Security, Personal Security, Communal Security and Political Security) [7] [67].

In the aftermath of a disturbing detonating event, citizens tend to use technology

platforms such as microblogs to share crisis-related messages [67].

The information buried in these posts become a valuable asset that discloses what people feel, exposing ideas that range from sympathy or emotional support to disruptive suggestions that may create social instability [68].

This hidden context and the associated metadata can reveal the beginning of a crowd reaction and unveil the fragile internal balance of the affected state. Detecting when a critical mass of individuals feel "so" connected with that social stimuli represents a core challenge.

According to [69] when individuals are in a fully engrossed or fixated state, generate a measurable metric, "engagement". Engagement is the consequence of interest or disinterest towards a target. Hence, engagement is fully connected to a crisis event because the people who are dealing with a disturbing incident are more vulnerable to a disruptive groupthink (cognitive closure) [70].

Engagement is a multidimensional concept that comprises emotional and behavioural dimensions [71]. In light of social media and for this work, the **emotional component** refers to the private state of individuals that is mirrored when messages have been spread over the internet (emotions or opinions).

The second element (**behaviour**) focuses on capturing the ways in which the balance of Human Security aspects is disturbed by the triggering on an incident.

In line with these concepts, the **emotional** and **behavioural** components may enable the analysis of the affected Human Security facets and the nuances of the emotional states.

A disruptive situation has to be analysed over a short-term time frame, to study how people express their feeling of belonging and relatedness towards a situation as described in [72].

We propose the term "**Social Media Connectedness**" (SMC) to refer to this phenomenon. For the work described in this chapter, SMC represents the length of time (hours or days) where a mass of individuals felt involved and engaged towards a cause.

This chapter puts forward the *hypothesis* that **SMC** combined with the **emo-**

tional and **behavioural** components can constitute the main elements of an analysis that reveal when a society is headed towards a critical national security event, due to individuals having reached a tipping point and the state potentially collapsing.

The next section presents the analysis that we have conducted to provide a basis to this hypothesis. For this analysis, the emotional component is modelled using the Global Polarisation index [73], while the behavioural part is captured by the Human Security Impact parameter [7].

3.3 Analysis

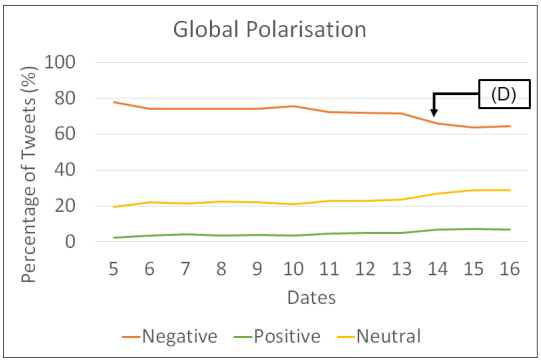
For the experimental investigation tweets from four different national contexts and dissimilar triggering incidents were collected as shown in Table 3.1.

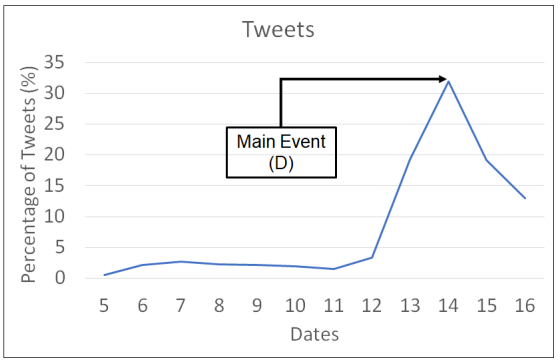
The data corpus was built by extracting tweets linked to trending hashtags, using the historical Tweet API. As a result, two data clusters were created to separate the disruptive from the non-disruptive events.

All the disruptive cases were selected because the society reached a tipping point that led to riots, unrest and violent events (see Figure 3.2). In the disruptive cases, we have included the Syrian conflict. Although this is not a case of directly predicting social unrest, it provides important and useful insights into society's reaction and state, as a result of violent events.

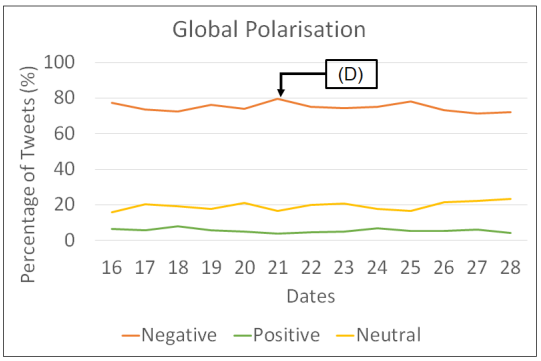
The analysis focuses on examining the data before such tipping points in order to investigate the different key parameters for the proposed Alert Mechanism.

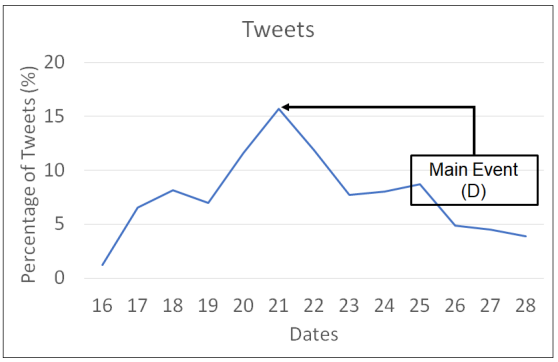
Tweets are a means of communication in the digital era, and a retweet is the mechanism to spread a message that because of its viral content is spread to new audiences for the purposes of engagement [74].



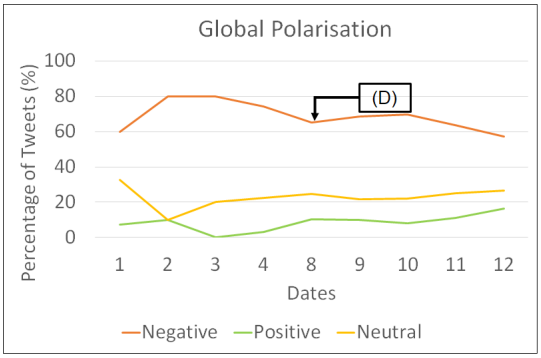


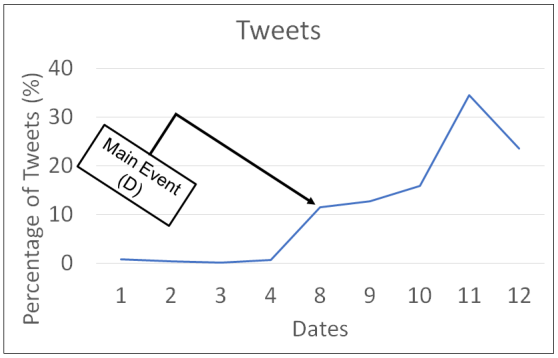
(a) Aleppo (December 2016)



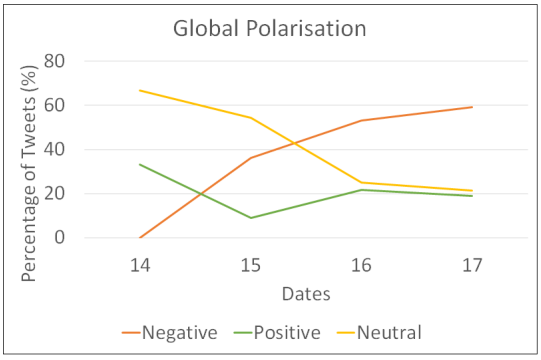


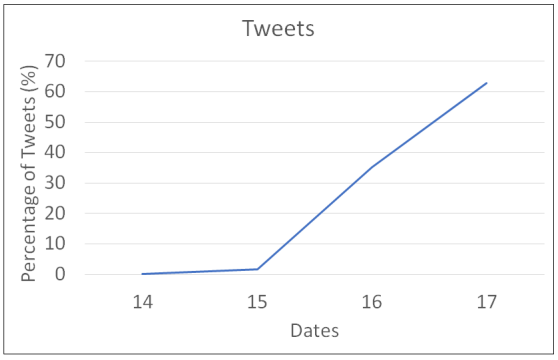
(b) Libya (February 2011)





(c) Egypt (February 2011)





(d) Drawing while Black, USA (September 2017)

Figure 3.2: Analysed Datasets

National Security Crisis	Description	Disruptive	Detonating Event	Main Event	Number of Tweets
Fall of Aleppo, Syira (December 5th - 14th, 2016)	Military conflict	Yes	Russia and China veto a UN Security Council resolution calling for a seven-day ceasefire in Aleppo (December 5th, 2016).	Violent activities (December 14th, 2016)	175,934
Conflict in Libya, Libya (From February 16th - 28th, 2011)	Social unrest	Yes	The Libyan leader, who has ruled over the country for more than four decades, voiced support for Mubarak during the Egyptian crisis (Feb. 14th,2011)	Libyan protests (February 21st, 2011)	62,791
Conflict in Egypt, Egypt (February 1st - 12th, 2011)	Social unrest	Yes	H. Mubarak announces in a televised address that he will not run for re-election but refuses to step down from office (February 1st, 2011).	Egyptian protests (February 8th, 2011)	7,546
Drawing while Black, USA (September 14th - 17th, 2017)	Artistic event	No	An artist started the hashtag #DrawingWhileBlack (September 14th, 2017).	No main event	3,987

Table 3.1: Disruptive and Non-disruptive datasets

For this work, tweets written in English that have been retweeted at least once were selected to construct a new data corpus as described in [67]. As a result of this process, the Disruptive and Non-Disruptive datasets were condensed as shown in Table 3.1.

3.3.1 Global Polarisation

After selecting retweets, a cleansing process was performed to remove stop words and punctuation. Therefore the disruptive and non-disruptive datasets were analysed to measure the mood states and classify them into three categories: positive, negative and neutral as described in [67], by using a lexicon-based approach.

The Polarisation procedure discloses the first clue as it unveils which set of sentiments had a predominant role and eased the detection of elaborate disagreements towards a selected topic.

As illustrated in Figure 3.2, disruptive incidents showed that negative polarisation fluctuated above 60% of total related tweets before the main event, whereas the non-disruptive dataset (see Figure 3.2 (Drawing while Black, USA)) had gradual increments over time, but the Global Polarisation index remained below 60%. This polarisation index revealed that disturbing incidents tend to hold a stable negative perception, while a non-disruptive event presents an irregular pattern.

3.3.2 Social Media Connectedness

As described above, the SMC process is focused on quantifying the length of time (hours or days) where a mass of people feel connected towards a cause, and a continuous dialogue amongst citizens has begun.

However, spotting those behavioural patterns is non trivial, but a starting point is by classifying the tweets into the ten categories of Human Security aspects, as defined by the United Nations [7], namely Defence, Economy, Environment, Government, Information, Health, Life, Transport, Public Order and People.

For this purpose, a multiclass classification model was trained using the architecture shown in Figure 3.3. As a preliminary step, text coming from a specialised

dictionary by the UK Local Government Association [66] that handles words related to human security variables was transformed using sentence embeddings which were used as the input for the neural network. The dictionary was enriched by getting synonyms in the Wordlist lexical database to get a trustworthy wordlist, as described in Chapter 2. Then, three fully connected layers were used as part of the architecture. Finally, the output layer had ten neurons which is in line with the number of human security components. This multiclass classification model was used to classify the tweets from the disruptive and non-disruptive datasets, and the percentage of each Human Security component was calculated per day.

As described above, Human security components are critical indicators to maintain the stability of a state, but understanding the relationship amongst them becomes a significant task. A Granger causality analysis was performed on the disruptive datasets, where similar to [75], this analysis was used to examine whether one Human Security aspect has predictive information about the other one. This approach was adopted as Granger causality between two variables cannot be interpreted as formal causation [75].

Human Security Components	**p-value**
Business -▷ Defence	4.07E-06
Health -▷ Defence	0
Defence -▷ Environment	0.03914484
Business -▷ Health	0.02018019
Defence -▷ Health	0
Public Order -▷ Information	0.04565287
Defence -▷ People	0.14683295
Environment -▷ People	0.58523553
Defence -▷ Public Order	0.07491134
Environment -▷ Public Order	0.02676013

Table 3.2: Statistical significance (p-values) of bivariate Granger Causality correlation amongst Human Security components

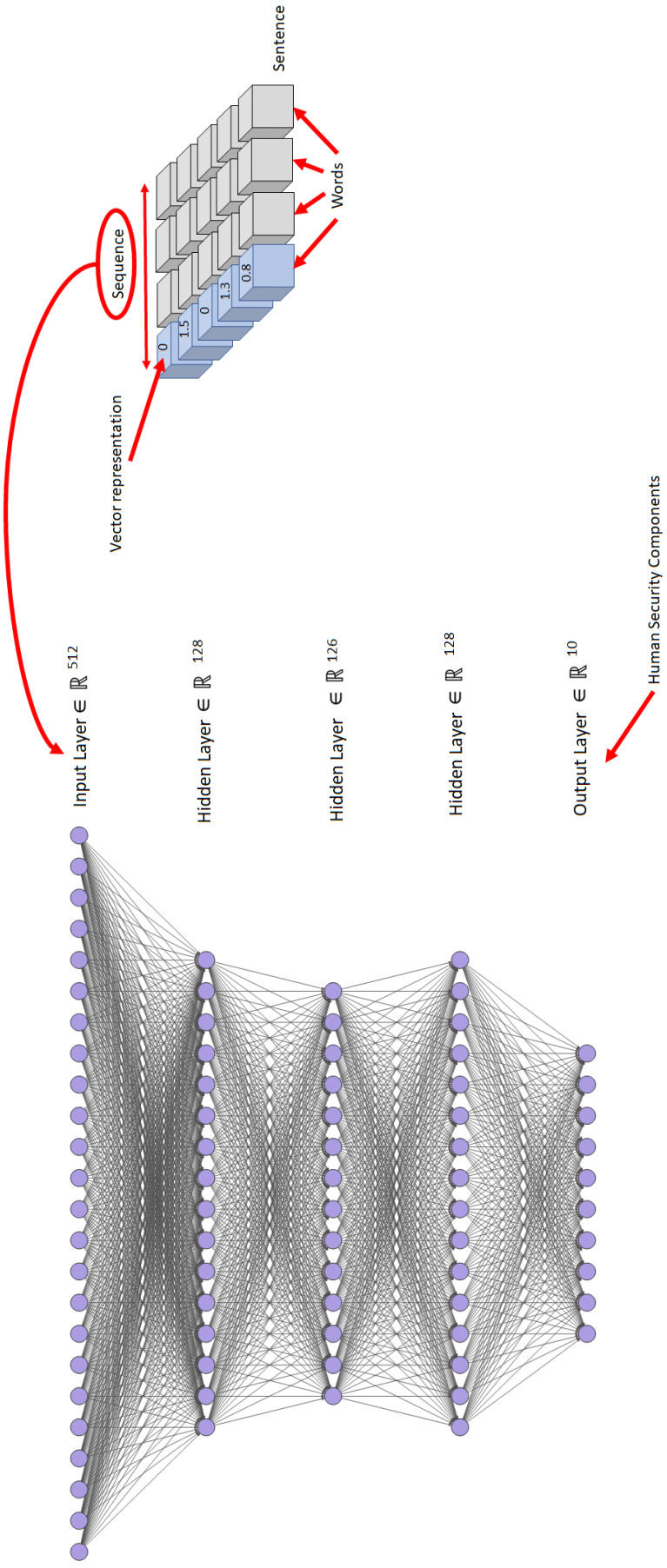


Figure 3.3: Architecture of the Multiclass classification model for categorising Human Security Components.

Based on the results of the Granger causality analysis (see Table 3.2) it can be observed that Defence - People, Environment -People and Defence - Public Order had the highest Granger causality relation (p-value > 0.05), whereas the rest of the variables did not present a significant correlation.

Moreover, before the tipping point (significant situation) has been reached there is a crowd reaction, observable as an activity ramp-up [2]. Therefore, it is required to examine which of the variables with the highest Granger causality relation increased or maintained a stable behaviour over time.

Hence, People, Defence, Environment and Public Order were investigated further as shown in Figure 3.4, Figure 3.5, Figure 3.6 and Figure 3.7, respectively. It can be observed that the variable People behaved consistently since it stayed above 10%, while the other parameters demonstrated a more random behaviour.

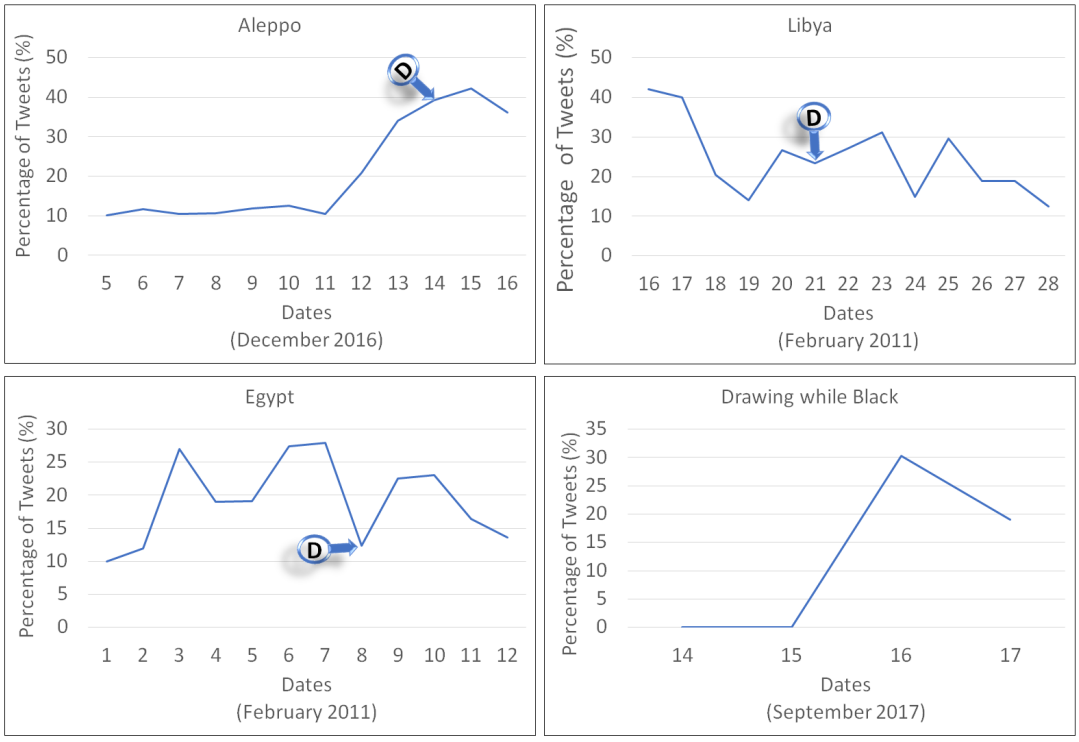


Figure 3.4: Percentages of one Human Security Component (People) across three disruptive cases (Aleppo, Libya and Egypt) and one non-disruptive case (Drawing while Black, USA).

This result is clearly linked to the fact that national security is a people-centred topic [7], and it suggests that individuals were using words related to human beings

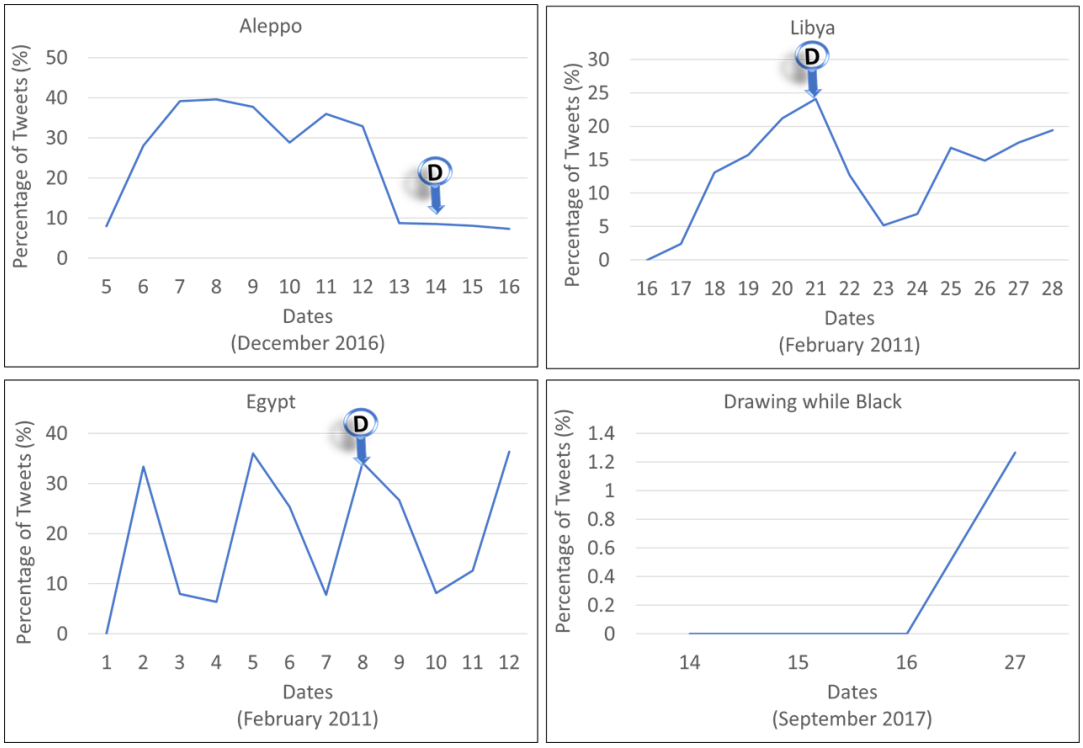


Figure 3.5: Percentages of one Human Security Component (Defence) across three disruptive cases (Aleppo, Libya and Egypt) and one non-disruptive case (Drawing while Black, USA).

to invite other groups to join the groupthink. Some indicative examples of real tweets are: "Hate groups are active" and "The war is against vulnerable people".

Therefore, the component "People" can be considered as an important indicator of intergroup behaviour. The next step of the analysis was focused on creating a model to correlate the behaviour of this component, based on the negative perception of the rest of the Human Security components.

The creation of this model is an important step because high values for "People" is not indicative of a disruptive incident, as non-disruptive events such as a sports game or a music concert would lead to a similar sharing of messages that contain words related to human beings.

Three popular models were selected and trained (Gradient Boost Machine, Random Forest and a Long-Short Term Memory model (see Figure 3.8).) by using the three datasets described above (Libya, Syria and Egypt). In each case, the response

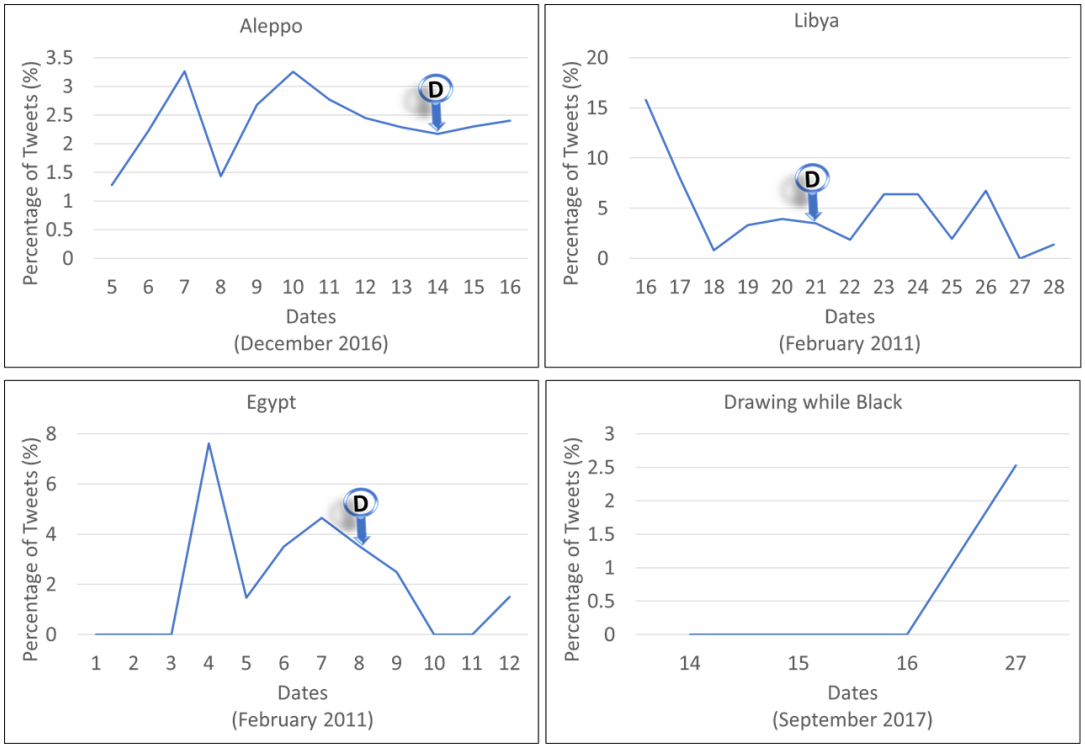


Figure 3.6: Percentages of one Human Security Component (Environment) across three disruptive cases (Aleppo, Libya and Egypt) and one non-disruptive case (Drawing while Black, USA).

variable (People) was labelled by setting it to 1 when it was above 10%, the threshold identified in Figure 3.4, and 0 when it was below this threshold. The remaining Human Security aspects were used to input parameters to the model.

The LSTM model was selected because the prediction of civil unrest events can be seen as a time series prediction problem and the alteration of human security components change over time as the incident escalates. Moreover, such a model is well suited to categorise, process and make forecasts based on time series information and predict near-future events [41].

The accuracy of each model was calculated by using the AUC metric (Area Under the Curve), and the results are shown in Table 3.3. Consequently, the Deep Learning Model presented the best performance and its relative variable importances are shown in Table 3.4.

These results suggest that individuals can get involved towards a national security cause when negative messages related to **defence**, **health** and **government**

Model	**Accuracy**
Random Forest	74.47%
Gradient Boost Machine	76.98%
LSTM	94.60%

Table 3.3: Model Accuracy

Human Security Component	Importance (%)
Defence	21.05
Health	18.76
Government	16.74
Information	16.6
Environment	12.6
Public Order	7.38
Life	6.87

Table 3.4: Human Security components influence

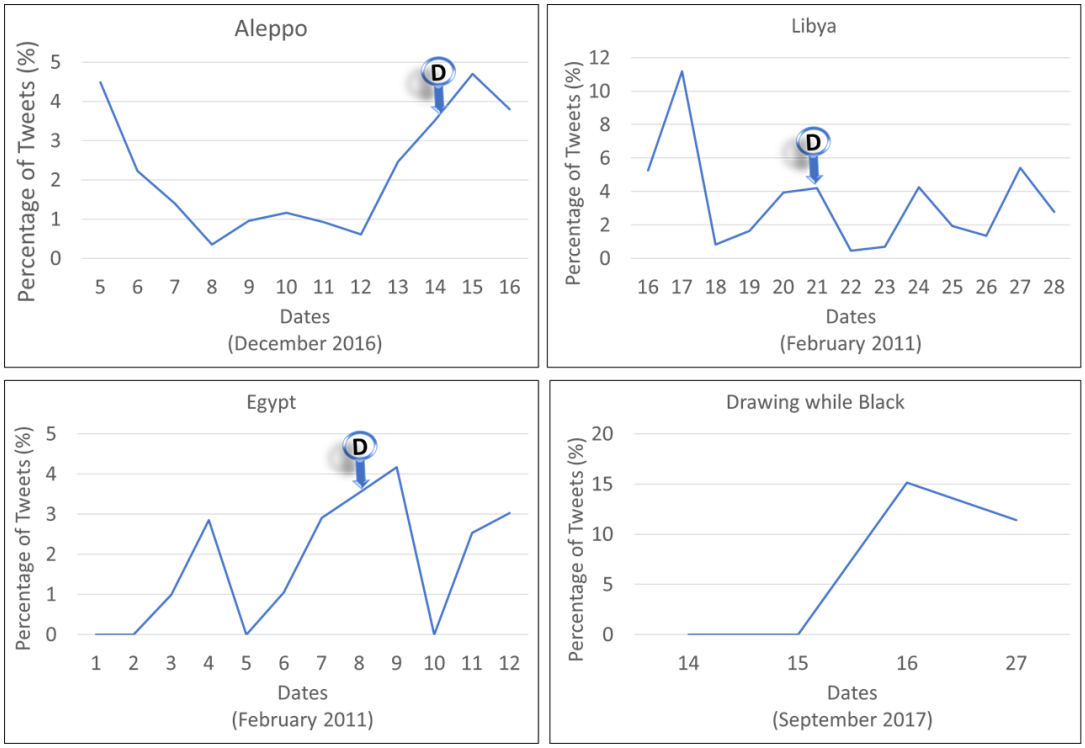


Figure 3.7: Percentages of one Human Security Component (Public Order) across three disruptive cases (Aleppo, Libya and Egypt) and one non-disruptive case (Drawing while Black, USA).

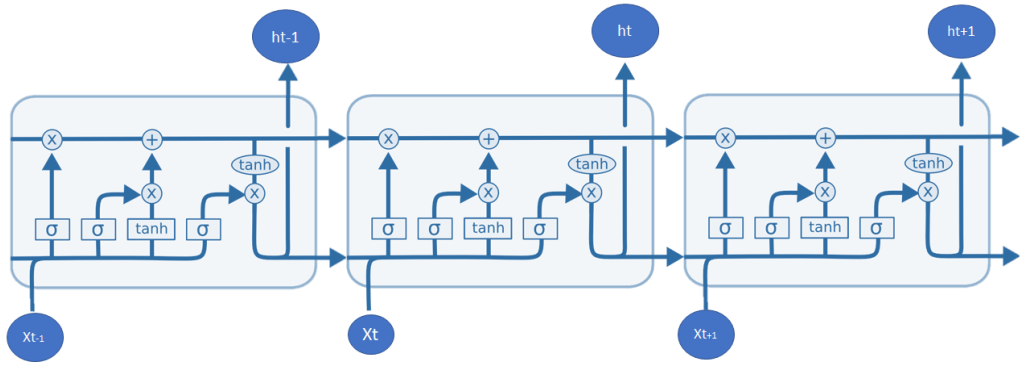


Figure 3.8: LSTM architecture used for the Alert Mechanism.

have been conveyed.

As described by [2] real-world events have increases in activity due to external causes also known as an "exogenous" variable. By contrast an "endogenous" variable is not related to a real event, because this kind of element is originated and spread within the social media environment.

As negative messages had the predominant role, in this case **"defence"**, **"health"** and **"government"** can be considered as exogenous variables since they work as an external cause, while the variable **"information"** can be considered as an endogenous component, as it includes words related to technology, and these set or words are not linked to the disruptive situation.

3.3.3 Human Security Impact

Violence, blood, injuries or medicines are some terms that can be found when mining unstructured data (tweets) after a detonating event. The variable importances, shown previously, indicate that **"Defence"** is the primary aspect that citizens shared while a disruptive event is being organised, which is why in this work the Human Security Impact will be based on this specific component.

Figure 3.5 illustrates that while "Defence" had a variable pattern in the studied disruptive incidents, it always measured above 5%. Whereas in non-disruptive events it remained below 1.5%, despite a burst of activity. Hence, the threshold for the measurement of "Defence" is set to negative posts above 5% of total, to indicate that Human Security has been compromised.

3.4 The Proposed Alert Algorithm

Based on the analysis and the results described above, the proposed Alert Mechanism is shown in Algorithm 2.

The mechanism has three component phases, namely Global Polarisation, SMC and Human Security Impact. In the first phase, tweets are ingested and processed to get the sentiment polarisation. This step unveils the real nature of the event because when negative opinions are present, a clear proof of unhappiness towards an incident begins to flow.

If the polarity outcome exceeds a certain threshold (T1) then the spotted incident can be considered a likely threat and the second phase will be initiated.

The second step quantifies the length of time (hours or days) where a mass of

```
Data: Tweets
Result: Trigger an Alert
/* T1= Negative Sentiments Threshold; T2= Time span (days/hours); T3=
   Human Security Component Threshold                                  */
begin
Global Polarisation (GP)
if GP >= T1 then
    Social Media Connectedness (SMC)
    if SC >= T2 then
        Human Security Impact (HS)
        if HS >= T3 then
            Trigger an Alert
        end
    end
end
```

Algorithm 1: Alert Mechanism

people feel attracted towards a cause, and afterwards, the result will be analysed in the light of a different threshold (T2) to decide whether the set of disruptive beliefs have been on the trends site for a long time.

The third phase deals with the analysis of the Human Security Parameters, to decide if the mass of people were highly engaged, namely they were above a predefined threshold (T3) and are heading towards a tipping point in which case an alert will be triggered.

From the results described in Section 4.3, T1 was considered as critical value when it was above 60%, whereas T2 was set to four hours since a topic can be considered as a popular one when it was on trends site for more than four hours (a figure consistent with the analysis provided in [76]), and T3 was considered as significant when the human security component "Defence" was above 5%.

It should be noted that the lower the thresholds are, the earlier the mechanism will issue an alert; however, that would also increase the probability of false positive outcomes.

In practice of theory, the alert mechanism could utilise a learning component to allow T1, T2 and T3 to be dynamically adapted and calibrated to reduce false

positives in different contexts.

3.5 Validation

To demonstrate the validity of the proposed mechanism, we have utilised it in the context of one additional case related to a disruptive incident namely the Ferguson Riots, USA.

The purpose of this exercise is to verify the following: if the proposed mechanism had been available during that event, with the prescribed threshold values, would it have issued an alert, and if yes, when would the notification point occur?

The Ferguson case examines the events in 2014 in the USA, where protests and riots began after the fatal shooting of a man called Michael Brown by police officers.

The analysed time span comprises from November 11th to 29th, 2014 and as Figure 3.9-I illustrates two critical situations need to be outlined, the former is when the governor declared the state of emergency and the second one when the grand jury decided not to indict the officer.

In this case, the Alert Mechanism was used to analyse the first critical event, from November 12th to November 17th, 2014 before the declaration of the state of emergency took place (see Figure 3.9-II).

Therefore, the Global Polarisation index was calculated from November 12th – 16th, 2014, and it shows that negative sentiments remained above 60% (see Figure 3.9-III). This result suggests that individuals were conveying messages with more negative emotions.

Secondly, SMC was calculated by using the Deep Learning model described above, and it reveals that five days before the main event, people were "engaged" with the incident for 22 out of 24 hours per day (see Figure 3.9-IV).

Based on the analysis in [76] a topic is considered as a very popular one when it was on trends site for more than four hours. Consequently, the outcomes described above indicate that individuals were highly involved before the governor declared the state of emergency.

Finally, Figure 3.9-V detailed that defence levels increased from November 13th

(D-4) and remained above 10%.

From the above, if this mechanism had been utilised when these events occurred (November 12th -17th, 2014), an Alert would have been issued **four days** before the main incident - on November 13th.

3.6 Conclusion

This chapter has introduced a new algorithm and mechanism that can issue alerts to help relevant authorities and stakeholders anticipate major societal disruptions that constitute national security threats. We have identified three indicators that can be used as the core parameters of such an alert mechanism: Global Polarisation, Social Media Connectedness and Human Security Impact. These indicators can reveal the real nature of the event and whether a society may be heading towards a situation where the stability of the state may be affected.

The validity and robustness of the proposed algorithm has been demonstrated in a disruptive event, namely the Ferguson riots in the USA. Future work will utilise larger and diverse datasets for validation, leading to integration in the proposed decision support system (see Figure 3.1).

It should be noted that continuous training of the Alert Mechanism can recalibrate the required thresholds (T1, T2 and T3), but decision-makers are the primary stakeholders that can choose and evaluate the trade-offs. There are costs associated between high and low sensitivity that can be determined by considering ignoring or acting on an alert.

Slang expressions, offensive content and hate expressions are some language nuances that individuals are using to convey their feelings, which is why such thought processes will be considered in future work to expand and improve the polarisation analysis.

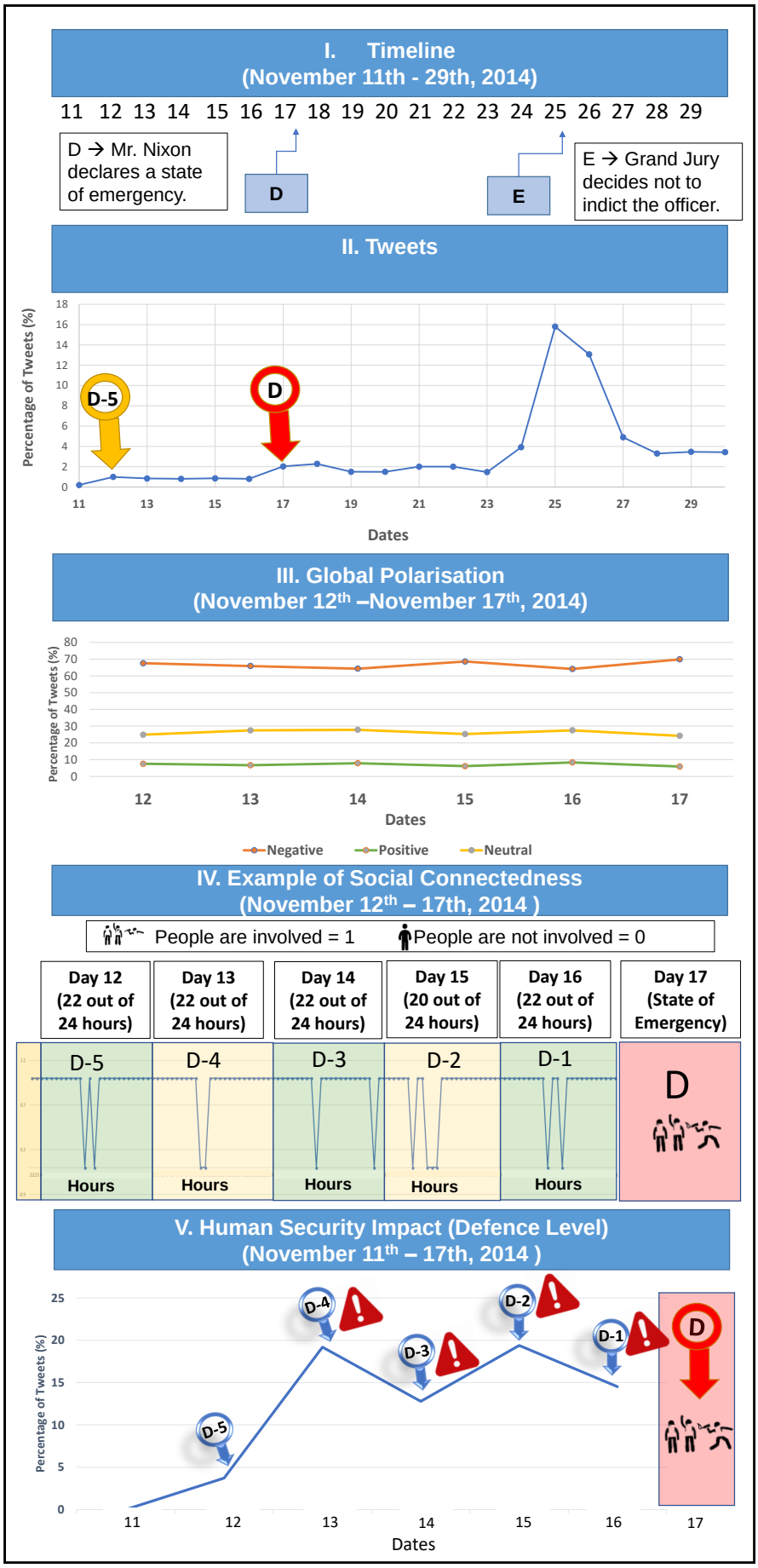


Figure 3.9: Ferguson Riots Analysis (November 2014).

Chapter 4

Web Insights for National Security: Analysing Participative Online Activity to Interpret Crises

4.1 Introduction

A crisis is an inflection point where the typical social structure, norms and values are interrupted [2] and as a result, the society deals with a disruptive situation that affects and undermines the capacities of the state.

In the digital era, the affected population convey their feelings, emotions or needs by using participative online communication channels that enable the flow of the information at an accelerated pace. Therefore, individuals tend to share and create content [2] through dissimilar applications that range from social networking services to websites. The information produced in such content may reflect core aspects of the society such as the way people are facing the event, or emotional indicators that show intentions that may lead to increase or extend the crisis over time.

One way to understand such behavioural indicators is by analysing the information that has been added as a complement while posting and that can be clustered into two groups. Firstly, the static pages embodied into websites and secondly mes-

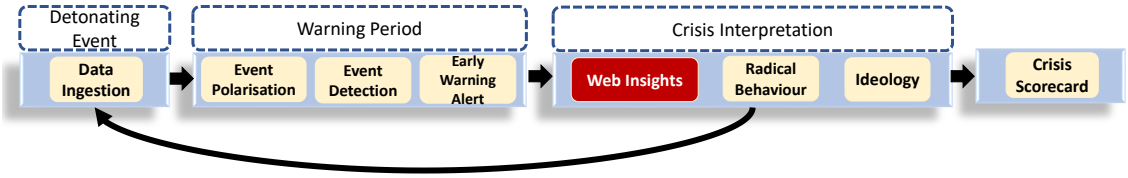


Figure 4.1: Conceptual Framework for Social Movements Analytics for National Security

sages from different social networking services that include personalised comments that tend to become viral.

The importance of the groups underlies in the fact that both websites and the messages from dissimilar social networking services can be disseminated by a crowd. Hence those aspects can provide useful insights to interpret a crisis and determine whether national security is compromised.

As described in Chapter 3 a holistic framework aimed at examining national security threats through social media analysis was detailed, and it comprises three core stages namely Detonating Event, Warning Period and Crisis Interpretation, as depicted in Figure 4.1.

During the first and the second stages -Detonating Event and Warning Period-, messages are collected and processed, respectively to spot which national security variables were affected and afterwards, an alert is triggered based on predefined thresholds to represent when a likely threat tends to unbalance the security of the state. In Chapter 4 we provided a description of the algorithm used for the alert mechanism and demonstrated its validity in a disruptive case namely the Ferguson riots (the USA, 2014).

Once an alert is issued by the system, the third phase is initiated, namely Crisis Interpretation. This phase is meant to provide the relevant stakeholders deeper insights about the nature of the crisis and support them in their effort to deal with the unfolding situation. This stage of the system assimilates what individuals are expressing through the different digital communication channels by using a set of computational techniques and transform the data into digestive pieces of information that decision-makers can use as valuable assets to draw insights and create a road map for addressing the crisis.

As part of the Crisis Interpretation process (see Figure 4.1), this chapter is focused on the Web Insights step, which works as a sub-process that analyses the participative online channels described above to unveil meaningful insights that enable the elucidation of the disruptive situation, through three main aspects. Firstly, the escalation of the crisis over time. Secondly, the interpretation of the information that the main actors have published (social networking services, information outlets, non-governmental organisations and independent websites). Thirdly, to estimate whether the crisis has turned violent.

Several different efforts and approaches for extracting data and knowledge from the web (Web Scraping) have been proposed and developed (e.g. [77], [78], [79]). However, to the best of my knowledge, there is no integrated methodology to utilise the data that can be extracted from the web for national security.

4.2 Background and Related Work

The Internet has become the main path where the information flows and such characteristic entails that data comes as a deluge. This can create a chaotic environment when dealing with a crisis event since individuals use different channels such as social media to convey their messages and in such a way to reach bigger audiences. In such situations, people need to convey as much information as possible in a single message, which is why they include additional data such as short URLs which provide information in two different ways.

The first one refers to the websites that contain detailed information about the issue individuals are facing, whereas the second way appertains to messages from various social networking services that embody what people feel or think about the disruptive situation.

The analysis of both data expressions requires different perspectives due to the former (websites) involving mining the content of numerous websites that have been added to the social media messages, whereas the second one analyses short text messages. The extraction of data from the web and its analysis can be a big challenge because the information within those websites follow a structured or semi-structured

format [80] and require different computational techniques. These challenges increase during a crisis event as many stakeholders publish their sites with the aim of sharing, conveying or spreading news or ideas amongst people, and such a significant volume of data, hinders the selection of those websites that publish relevant information to understand the crisis from the ones that do not.

When a disruptive event has been unfolded, emotions, opinions and news can gain resonance and increase the volume of messages and websites that embody what people are facing by expressing concerns about the interruption or unbalance of those elements that rule a state and that are closely linked to the national security components namely Economic Security, Food Security, Health Security, Environmental Security, Communal Security and Political Security [7]. However, understanding such interruptions require an analysis of the Instruments of Power that run across the political, military, economic, social, informational and infrastructure spectrum [81].

Both the instruments of power and the national security components consider the same components, and according to [81] a disruptive situation is present when the number of security components increases over time, called Horizontal Escalation. By contrast, Vertical Escalation only represents the intensity of such aspects, see Figure 4.2. For this analysis, the information extracted from the different web resources will be classified into the various National Security components and in such way enable the detection of an escalation or de-escalation of the event over time.

Moreover, a disruptive event can be spread at several locations within the same country, and spotting such venues enables a more accurate way to construe the crisis. According to [82] there are two forms to cluster a disruptive event namely city-level and widespread events. The former describes when an event occurs in the same state or city, whereas the second one illustrates when the incident reached several locations across a state or city.

There is a large set of questions a competent stakeholder may ask to drive their decision making during a potential National Security crisis. In this paper we focus on the following three:

- Q1.- Do national security components horizontal escalation over time?

- Q2.- Do Social Networking Services, NGOs and the rest of the web resources publish information that reveals disruptive activities?
- Q3.- Have social disruptions reached expressions of violence?

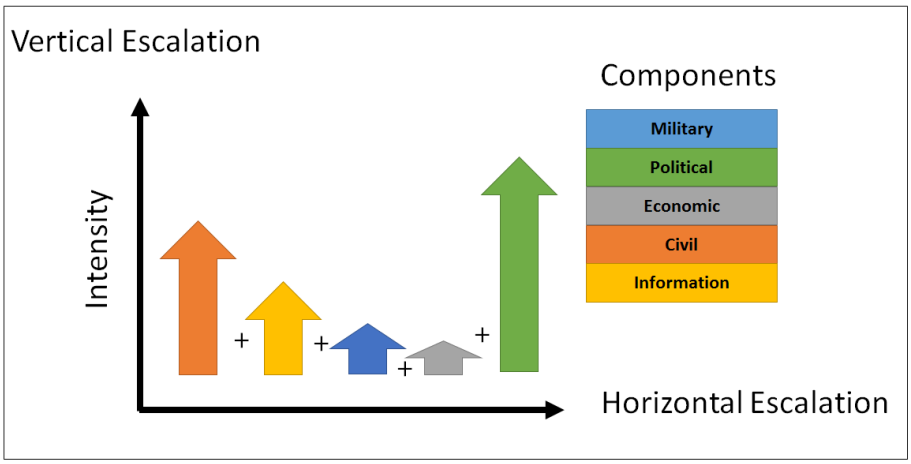


Figure 4.2: Instruments of power. Adapted from [81]

4.3 Methodology to Analyse Participative Online Activity (RQ3)

The proposed approach for extracting insights from the web related to National Security is illustrated in Figure 4.3. It consists of six stages, namely URLs Extraction, Expand URLs, Entity Extraction, Entity Classification, URL Identification and Analytics and Insights, that as a whole contribute to analyse participative online sites and to interpret a crisis.

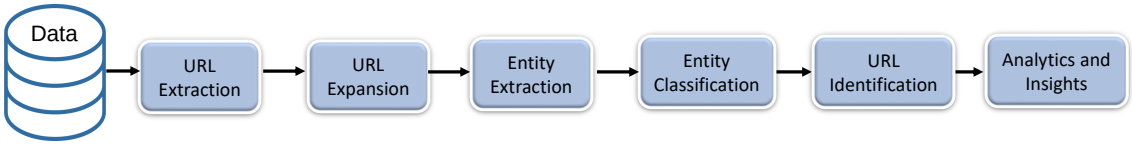


Figure 4.3: Proposed methodology workflow. Arrows depict dependency and sequence

4.3.1 URL Extraction

Twitter is a social networking service on which people post and interact by using messages limited to 280 characters; but to add more information to those messages, users include links to web-pages, blogs or other social networking services, to reinforce or complement what they need to express.

However, to avoid lengthy links individuals condense them by using external services such as Twitter's t.co, Google's goo.gl, Facebook's fb.me or bit.ly. Therefore, the first step of the proposed methodology is focused on extracting all the tiny URLs embedded into the tweets.

4.3.2 URL Expansion

As the second step, URLs need to be expanded to extract the complete reference of the web resource, but the collection of the unshortened URLs will be limited to those services that do not require to be logged in. As a result, the expanded link will follow a two-pronged path. Firstly, it will be used to mine the content of the web address, and secondly, it will allow the identification of the hostname.

4.3.3 Entity Extraction

As described in Section 4.2, when dealing with a National Security issue a significant task lies in detecting whether the disruptive event is affecting a single location (City-level events), or if it is being spread to different cities (Widespread events). Moreover, a core aspect is to know which critical infrastructure must be protected in the affected area and which organisations are publishing the information across the Internet (public service broadcasters, television channels or newspapers).

In line with this idea, in this thesis the term entity will refer to the former three aspects namely, locations, critical infrastructure and organisations. However, to find out which entities can be involved, three comprehensive dictionaries can be created.

The first one involves a list of human settlements where crisis events can evolve in the affected country. As described by [83] [84], human settlements follow a hierarchical structure, namely, Megalopolis, Conurbation, Metropolis, City, Large town,

Small town, Large village, Small village, Hamlet and Isolated dwelling.

The second wordlist includes the critical sectors that need special attention, such as emergency services, energy, financial services, government facilities, transportation systems, defence, nuclear reactors, communications and chemicals, as described in [85].

Finally, the third dictionary requires a catalogue aimed to cluster those organisations that create content for an end-user in specific contexts, such as broadcasters, television channels, multimedia mass media companies or radio networks.

The importance of the dictionaries described above represents a core aspect since information is constantly evolving, and new locations are created, or some organisations disappear without prior announcement; which is why one alternative is the usage of a knowledge base such as Wikidata or Wikipedia to produce comprehensive lists that can be updated continuously.

4.3.4 Entity Classification

In the previous stage (Entity Extraction), three specialised dictionaries were created (human settlements, critical infrastructure and organisations) by performing queries over the knowledge base Wikidata. However, when a violent event has been unfolded, information tends to be disseminated by different stakeholders (organisations) leveraged by their power to spread data [86]. As a result, organisations are dissected into four clusters. The first group includes Non-Governmental Organisations (NGOs). The second cluster comprises Information Outlets (such as BBC or Deutsche Welle). The third group involves Social Networking Services. The fourth group includes those websites created by individuals or organisations to share temporarily information derived from an incident, also called Independent Websites (see Table 4.1).

4.3.5 URL Identification

Once the entities have been classified, the next step focuses on identifying the hostnames, which is why the entities related to organisations will be matched to the

Table 4.1: Proposed Entities for Querying the Knowledge Base

Entities			
Megalopolis	Conurbation	Metropolis	City
Large Town	Small Town	Large Village	Small Village
Hamlet	Isolated Dwelling		

I. Human Settlements

Entities			
Emergency Services	Energy	Financial Services	Transportation Services
Defence	Nuclear Reactors	Communication	Chemicals

II. Critical Infrastructure

Entities			
NGOs.	Information Outlets	Social Networking Services	Independent Websites
Non-governmental organisation	Television Channel	Social Networking Service	
Non-profit organisation	Military Unit		
	Journalism		
	Radio Station		
	Headquarters		
	Miitary Alliance		
	Television Station		
	Broadcaster		
	Television Program		
	Television Network		
	Business		
	Newspaper		
	Daily Newspaper		
	News Magazine		

III. Organisations

extracted URLs.

This step performs a web scraping process aimed to extract two attributes namely title and content from the websites (NGOs, Information Outlets or Independent Websites), and the title when dealing with a Social Networking Service such as Twitter, Instagram, Google+ or Plag.

In addition, the URL Identification process explores the extracted attributes to find specific entities such as Human Settlements or Critical infrastructure in them, and as a result, it clusters and processes them separately; however, the volume of data may increase due to the fact that high-sensitive content tend to be conveyed at a faster rate and consequently become viral [2] [87], which is why a distributed full-text search engine can be used to address such scalability problem.

As shown in Figure 4.4, the URL identification process becomes an essential asset, as it clusters the URLs according to its hostname, and enable the identification of different entities (human settlements and critical infrastructure) within the title or content of the extracted URLs.

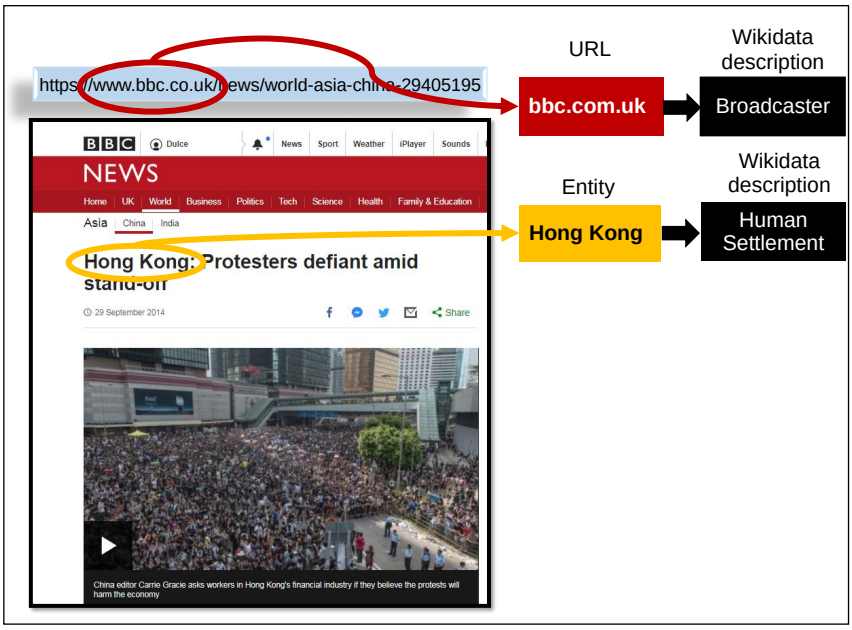


Figure 4.4: Extracting the hostname and entities from the BBC website

4.3.6 Analytics and Insights

Construing a crisis is not a trivial task since it requires to mould the data in order to extract useful insights that enable to unveil the situation the state is dealing with. As mentioned in section 4.2, the analysis is focusing on three questions related to the horizontal escalation of the National Components (Q1), the knowledge conveyed by web resources regarding disruptive activities (Q2) and the violent nature of the disruption (Q3). Below the approach is outlined to answer these questions.

1. *Horizontal Escalation of National Security Components*: Addressing this question requires to analyse and classify the data according to the National Security components described by [7] namely Economic Security, Food Security, Health Security, Environmental Security, Communal Security and Political Security, but such classifications require a set of words that can embody them.

   For this purpose, specialised wordlists such as those provided in [66] [88] can be used to feed a machine learning classification model. Moreover, as described in Section 5.3, to evaluate whether a disruptive event has intensified over time, a horizontal escalation analysis can be performed by examining the number of National Security components which have increased on a timespan.

   Therefore, time becomes a critical factor, which is why each National Security component has to be calculated per day. However, to evaluate the intensity of such escalation a baseline is required. This baseline will play an essential role because it will be used to normalise the National Security components in the analysed dataset and consequently evaluate its intensity level.

2. *Knowledge Conveyed by Web Resources*: Coping with this question (Q2) is especially important since both people and organisations use social media to convey messages or present breaking news, which is why processing those pieces of text represent a key element to disclose disruptive activities.

   A potential approach to address this challenge is to create a high-level summary of the content; such process extracts direct object dependencies within the data corpus by identifying intention phrases (see Figure 4.5). These expressions include verbs that denote the purpose to perform an activity, such

as unfold, occupy, assassinate, execute or immolate; the comprehensive study of verbs described by [60] can be used when analysing a disruptive event, as it defines a wide classification that includes verbs of psychological state, verbs of change of state, verbs of social interaction, verbs of contact by impact, verbs of communication or verbs of killing, see Table 6.5.

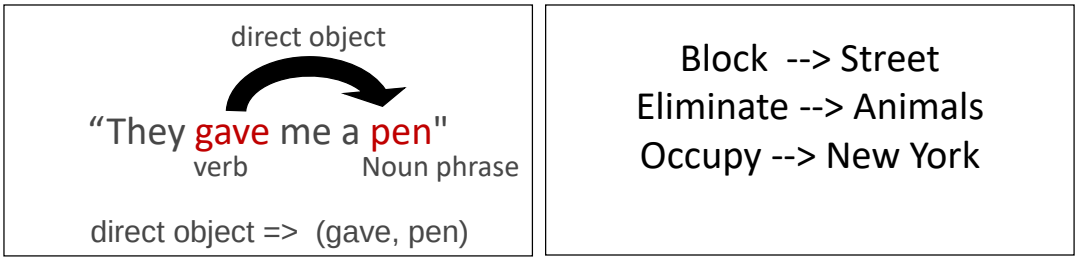


Figure 4.5: Phrasal structure and examples of intention phrases

Table 4.2: Example of verbs that can be used while analysing disruptive events. Adapted from [60].

Verbs of Psychological State	Verbs of Killing	Verbs of Change of State	Want Verbs	Verbs of Social Interaction
Occupy	Assassinate	Break	Want Verbs	Fight
Support	Kill	Tear	Desire	Meet
Tolerate	Liquidate	Unfold	Need	Visit

Verbs of Communication	Build Verbs	Verbs of Contact by Impact	Fill Verbs	Future Having
Say	Assemble	Beat	Block	Grant
Admit	Arrange	Bang	Bind	Allocate
Allege	Embroider	Slap	Bombard	Award

3. *Violent Nature of the Disruption*: The third question (Q3) deals with the concept of violence, and according to [82] there are some violence indicators (phrases) that may be present in a text and suggest that an event turned into a turbulent situation, see Table 4.3. In this case, the direct object dependencies extracted previously can be lemmatized and match to the violence indicators described above, to identify a disruptive situation.

Table 4.3: Violence Indicators. Adapted from [82].

Violent	Non-violent
Clashes with police (police using tear gas or high pressurewater hoses to disrupt a protest).	Threats of violence (yelling or cursing).
Clashes between opposing groups resulting in injuries.	Police arresting protestors.
Self-inflicted wounds (protesters sewing their mouths shut).	Hunger strikes.
Throwing hard objects which could cause injury or damage.	Throwing things that would not cause harm (eggs).
Hitting with sticks, bars, machetes, etc.	Brandishing sticks, bars, machetes, etc.
Burning tires, burning barricades, burning cars or buses, burning buildings.	Fireworks, blockades of streets.
Looting shops (where the shop is damaged).	Theft without damage.

4.4 Experiments and Validation: The Hong Kong Protests

To demonstrate the validity and robustness of the proposed methodology, a disruptive incident was selected namely the Hong Kong protests in 2014. These events started with a student strike on 22 September and developed to a protest outside the government headquarters on 26 September 2014 which escalated rapidly on 28 September with the beginning of a civil disobedience campaign. Consequently, for our analysis historical tweets were collected from September 26th to 30th by selecting hashtags considered as trending ones. The schematic view of the resulted data corpus can be seen in Figure 4.6.

As a preprocessing step, a sentiment analysis process was performed in a similar fashion to chapter 3 and described in [67], aiming at selecting those messages that exhibited the predominant role (the highest percentage). Figure 4.7 shows the result of this analysis, which depicts that the data corpus presents a negative polarisation. This suggests that individuals display a manifest disagreement towards the incident.

Once negative sentiments became predominant, they were used to feed the Alert Mechanism proposed in chapter 4 and detailed in [89], aimed to spot a critical state

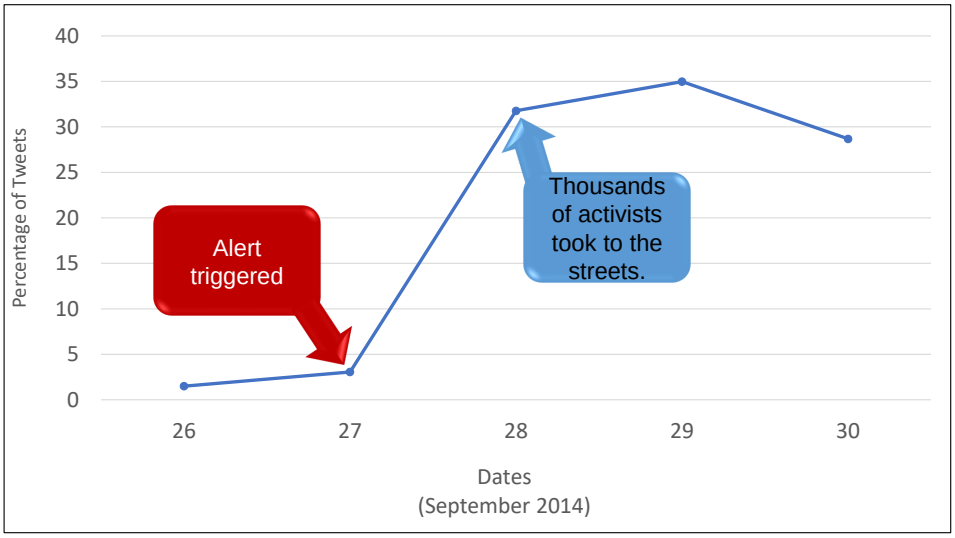


Figure 4.6: Tweets from the Hong Kong protest and the alert triggered by the system

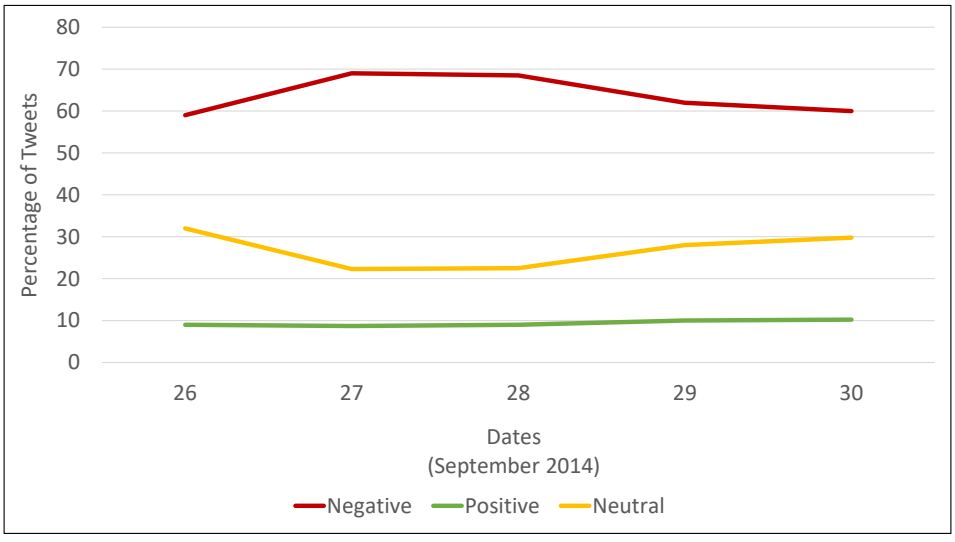


Figure 4.7: Sentiment analysis of the Hong Kong protests

or tipping point, where the society is heading towards a situation that compromised the national security, see Figure 4.6. Following the steps described in chapter 3, the mechanism triggered an alert on September 27, a day before thousands of people took the streets. For this study, this date represents a defining moment, since it splits the analysis into two phases. A previous facet to the tipping point (September 26) and the subsequent phase to the critical state (September 27 to September 30).

4.4.1 URL Extraction and Expansion

The interpretation process begins after the tipping point was detected. Hence, according to the proposed methodology, by performing the first Web Insights stage -URL Extraction- 108,524 web addresses were extracted. This figure becomes significant since 94% of the analysed tweets included a URL, as illustrated in Figure 4.8. Subsequently, all the shortened URLs were expanded as described in Section 4.3.2.

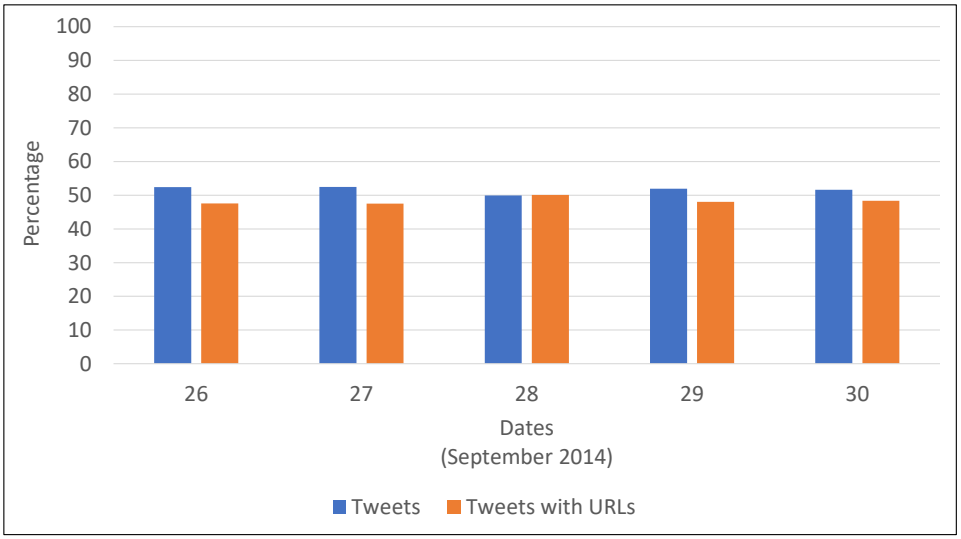


Figure 4.8: Tweets that contain URLs

4.4.2 Entity Extraction

For this step, three comprehensive lists were created based on the entities shown in Table 4.1. The first group corresponds to human settlements, the second one to

critical infrastructure and the last one to organisations. This process was performed by extracting the instances of the entities over the knowledge base Wikidata (e.g., Mong Kok is an instance of a human settlement), and as a result, 168,750 entities were extracted.

4.4.3 Entity Classification and URL Identification

After extracting and classifying the URLs, a web scraping process was performed to retrieve both the titles and the contents, as well. However, not all the web addresses were available due to a variety of reasons such as unauthorized access or because the site was moved permanently; but to retrieve the content of the latter, the Wayback Machine API was used [90].

Therefore, a core step relies on selecting those websites whose content unveil relevant information. In light of this idea, the content was considered relevant if it contained at least one of the entities related to human settlements or critical infrastructure, described above. Table 4.4 displays the total websites that contain relevant information.

Table 4.4: Websites with relevant content

NGOs	Information Outlets	Social Networking Services	Independent Websites
433	22,864	23,602	13,625

4.4.4 Analytics and Insights

As described in Section 4.2 there are three main questions to extract insights about.

1. **Horizontal Escalation of National Security Components (Q1):**

   The first question allows determining whether the crisis has escalated during a time span. In line with this idea, as a first step, a machine learning classification model was created aimed to classify the extracted titles from the

websites depicted in Table 4.4, according to the National Security components described by [7]. For this purpose a popular machine learning model was selected, the Gradient Boost Machine Model (GBM), which was trained by using the specialised lexicons [66] [88] described above.

Moreover, evaluating the intensity of horizontal escalation during a crisis requires a baseline that will work as a starting point and enable normalising the data. To create such a baseline, tweets from three different disruptive events were collected, namely the Conflict in Libya (Feb 16th- 28th, 2011), the conflict in Egypt (Feb. 1st -17th, 2011) and the fall of Aleppo (Dec. 5th -30th, 2016).

A sentiment analysis process was performed in all the cases to verify whether the negative tweets had the predominant role. These messages were then classified according to the national security components. Subsequently, the percentage of each National Security component was calculated per day, and the corresponding median will serve as the baseline (see Table 4.5).

Table 4.5: Percentages of the National Security components in dissimilar national contexts and their corresponding baseline

Event	Business	Defence	Environment	Government	Health	Information	People	Public Order
Libya	8.9	13.99	4.6	4.54	21.3	16	24.61	3.38
Aleppo	3.36	30.2	2.3	6.46	21.2	15.46	16.67	1.81
Egypt	11	22	1.71	13.77	10.43	17.19	19.17	1.5
Median	8.9	22	2.3	6.46	21.2	16	19.17	1.81

The intensity of the escalation/de-escalation of the national security components is computed by following equation 4.4.1.

$$IED = \frac{NSC - Baseline}{Baseline} \tag{4.4.1}$$

where:

IED = Intensity of the escalation/de-escalation.

NSC = National Security Component.

Figure 4.9 shows the horizontal escalation in four different instances namely Social Networking Services, Independent Websites, Media Outlets and NGOs.

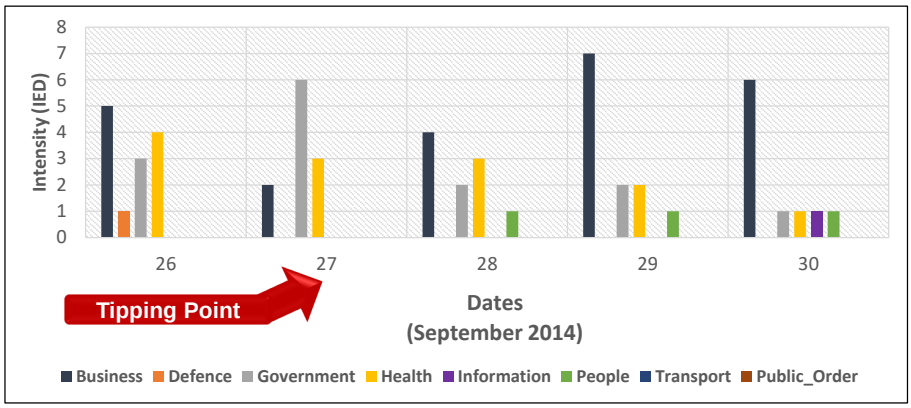
It can be seen that both the Independent Websites and the Information Outlets escalated horizontally when the alert was triggered (Sep. 27th) since they increased from three to four components and one to three components, respectively (see Figure 4.9-II and Figure 4.9-III); whereas the Social Networking Services provided significant information after the inflexion point (tipping point) was detected, as they changed from three to four components from Sep. 27th to Sep. 28th, and had another significant change on September 29th-30th because the components escalated from four to five (see Figure 4.9-I).

In addition, both the Independent websites and the Information Outlets published contents related to government, but with different intensities, which suggests that the former ones provided more detailed information about that subject to the people.

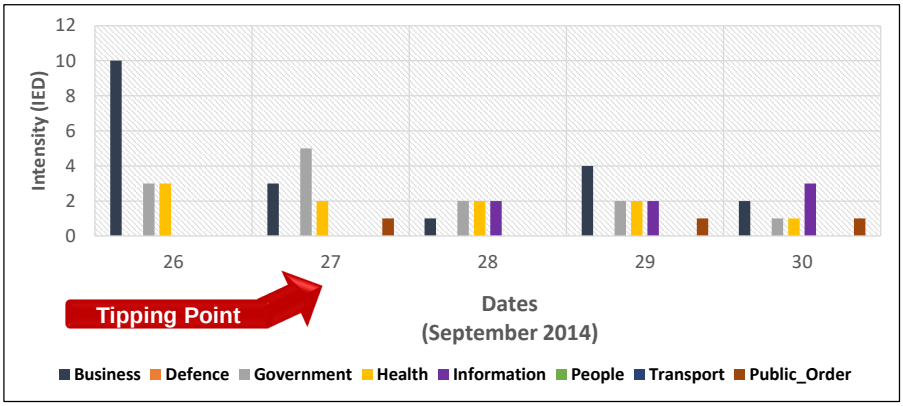
On the other hand, the NGOs published content related to the government but with higher intensity levels; however, horizontal escalation appeared twice. The first one was detected a day after the tipping point (September 28th) when the government component changed from zero to one. The second spot showed from Sep 29th-30th, when national security elements changed from one to two (see Figure 4.9-IV).

2. **Knowledge Conveyed by Web Resources (Q2):**

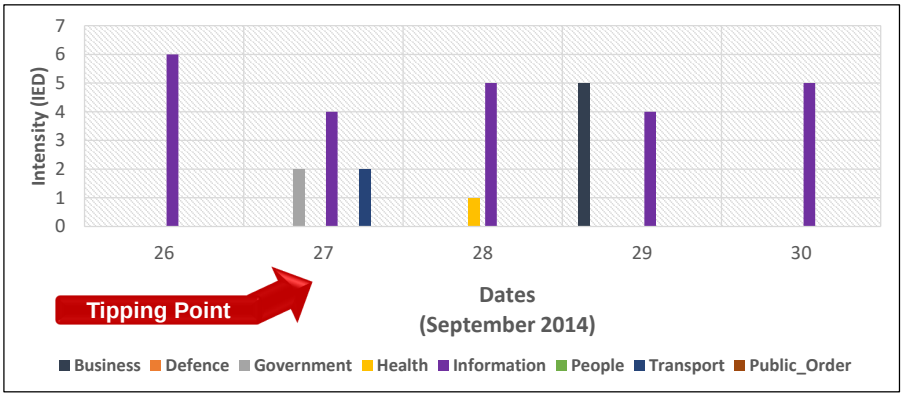
As a first step, the direct object dependencies from the different websites were extracted, aiming to identify intention phrases. In parallel, an intention wordlist was created based on the verbs described by [60] and shown in Table



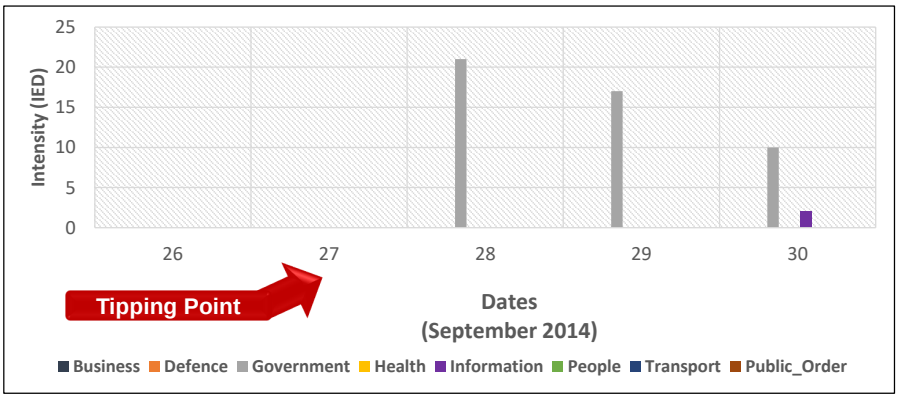
I. Social Networking Services



II. Independent Websites



III. Information Outlets



IV. NGO

Figure 4.9: Escalation of the National Security components during the Hong Kong protests (Q1).

6.5. Therefore, the direct object dependencies were lemmatized and compared with the intention dictionary previously created.

Table 4.6 shows the results from this step, and it can be seen that within Social Networking Services, individuals used the verbs of communication (say and read) to convey a message of disobedience from September 28th-29th.

Moreover, from September 28th, individuals showed their psychological state by expressing their intention to occupy different locations such as a metropolitan area (Wan Chai), a district (Kowloon), a business district (Admiralty) and a neighbourhood (Mong Kok). Also, people displayed their change of state since September 26th by publishing messages related to unfold a protest and a riot.

Regarding the Information Outlets and Independent Websites, most of the phrases correspond with the intention of blocking thoroughfares and building barricades.

3. **Violent Nature of the Disruption (Q3):**

To address this question, a dictionary of violent-related terms was created by considering the phrases proposed by [82], which were compared to the lemmatised direct object dependencies. As described in Section 4.3, a direct object dependency has two components; namely, a verb a noun phrase. The verb can disclose a violent activity such as spray or tear, and the noun phrase reveals the person, group of people or thing, that is, the recipient of the action of the aforementioned transitive verb.

Table 4.6 depicts that Independent Websites revealed a non-violent event on September 27th (when the system triggered an alert) since phrases such as blocking thoroughfares and erecting barricades were published on those web resources.

On September 28th,29th and 30th, the Information Outlets, NGOs and Social Networking Services disclose a violent event as individuals claimed that protestors were being beaten and sprayed with tear gas.

Table 4.6: Data Analytics of the Hong Kong protests (Q2 and Q3)

Social Networking Services				
(September 2014)				
Date 26	Date 27	Date 28	Date 29	Date 30
Unfold =>Protest	Unfold =>Protest	Unfold =>Protest	Kill=>Protester	Teargassed =>Protester
	Occupy =>disobedience	Read =>disobedience	Unfold =>disobedience	Continue =>disobedience
		Unfold =>Riot	Say =>disobedience	Beating =>Protester
		Trigger =>Riot	Reinforce =>Barricade	Unfold =>Wan Chai
		Impose =>Curfew	Unfold =>Barricade	Erect =>Barricade
		Build=>Barricade	Occupy =>Admiralty	
		Assembling =>Barricade	Occupy =>Kowloon	
		Blocking =>Thoroughfare		
		Occupy =>Mong Kok		
		Occupy =>Wan Chai		

Information Outlets				
(September 2014)				
Date 26	Date 27	Date 28	Date 29	Date 30
Want =>Suffrage	Support =>Protestor	Tear =>Protest	Blocked =>Thoroughfare	Teargassed =>Protester
		Blocked =>Thoroughfare	Blocked =>Gmail	Blocked =>Thoroughfare
		Tear =>Protest		

Independent Websites				
(September 2014)				
Date 26	Date 27	Date 28	Date 29	Date 30
Grant =>Protester	Join =>Protester	Block =>Thoroughfare	Block =>Throughfare	Block =>Throughfare
	Use =>Roadblock	Remove =>Blockade	Blocked =>Facebook	Build =>Barricade
	Block =>Thoroughfare	Defend =>Barricade	Defend =>Barricade	Protect =>Barricade
	Erect =>Barricade			March =>Placard

NGO				
(September 2014)				
Date 26	Date 27	Date 28	Date 29	Date 30
		Penetrate =>Barricade	Beat =>Protester	Remove =>Barricade
		Disperse =>Protester		Cut =>Barricade
		Sprayed =>Protester		Protest =>Jailing
		Pepper =>Protester		

4.5 Conclusion

When a crisis has been unfolded, people tend to use different communication channels such as Social Media to project their opinions, voice and feelings. However, to add more information and emphasise their posts, individuals include links to websites or other Social Networking Services, where similar ideologies are shared.

Analysing the information behind such web resources enable the extraction of useful insights to interpret the crisis and obtain a bigger picture of the situation by integrating computational techniques and high-level security concepts (National Security and Instruments of Power).

This chapter has introduced a novel methodology to dissect the information of those web resources and transform it into digestive pieces of information to construe a crisis through three main aspects. Firstly, the escalation of a crisis over time; secondly, the interpretation of the information that main actors such as Social Networking Services, Non-Governmental organisations, Information Outlets and Independent Websites have published; and thirdly, to estimate whether a crisis has turned violent.

The validity and robustness of the proposed methodology have been demonstrated in a disruptive event namely the protests in Hong Kong, 2014, where the results suggested that by analysing social networking systems, information outlets and independent websites, a crisis can be construed.

The validity and robustness of the proposed methodology have been demonstrated in a disruptive event, namely the protests in Hong Kong, 2014. The results suggested that the analysis of dissimilar digital sources of information contribute to identifying three main aspects. Firstly, spotting the escalation of the National Security components over time, which represents that the internal balance that maintains the stability of a state has been compromised. Secondly, singling out which entities are publishing essential data on the internet. Finally, identifying both violent a non-violent activity.

Chapter 5

Radical Behaviour

5.1 Introduction

Societal instability issues across the globe tend to disrupt the fragile equilibrium of the state. Researchers and the government are able to monitor the state of a country by attempting to track societal markers such as Economic Security, Food Security, Health Security, Environmental Security, Personal Security, Communal Security and Political Security [7]. This in-turn contributes to the detection of larger problems that would affect National Security.

However, the detection and interpretation of security instabilities is non-trivial, as threats are evolving and depending on the source or domain include their own specific nuances. New unregulated domains, such as cyberspace, make the early detection and mitigation of threats a complex task for most governments [91]. Such threats are known as Hybrid Threats as they are not just confined to the digital realm but can spill out onto the streets. These newly shaped threats are aimed to affect societies at large, not just armies [92] and employ both conventional and unconventional methods such as military, economic, or technological, which can be used by different actors to disturb the human security components and destabilise the state. By creating confusion, inciting fear, blurring the institutional decision-making process, or undermine the confidence in the government, as described in [93], Hybrid threats can shake the foundations of government and society.

Different instruments/tools (also known as Hybrid Tools [94]) can be used to

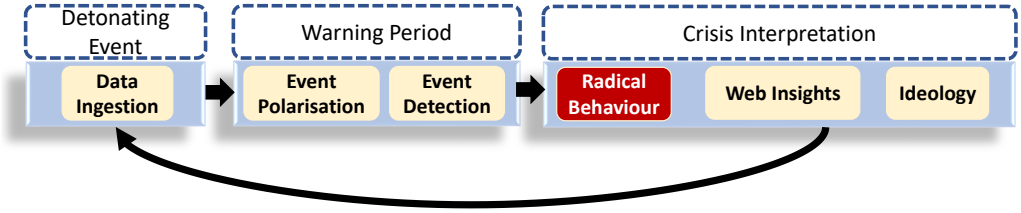


Figure 5.1: Conceptual Framework for Social Movements Analytics for National Security

amplify the impact of such disruptive activities on National Security such as Propaganda, Domestic Media Outlets, Strategic Leaks, Political Parties, Paramilitary Organisations and Social Media, among others [91].

The advent of the Internet has placed Social Media as a crucial asset to extract information from the virtual realm and strengthen a strategic analysis, since its core values lie firstly in the speed with which information travels, and secondly in the power that a set of clustered data offer unlike individual datum. This explains why the analysis of a set of tweets related to a specific topic unveil more information than a unique post on Twitter [95].

Social Media provides a platform that enables citizens to engage in discourse, and this plays a significant role in extracting the vox populi during a crisis event. Even during the lead up to such an event, the various text and contextual markers relating to National Security can be identified and mined to determine the extent to which the unfolding event will affect National Security [67].

Analysing and interpreting such information is a complex and challenging task, but it can provide useful insights that decision-makers can use to decide the best course of action to mitigate the disruptive situation. In line with this idea, as described in Chapters 3, 4 and 5, a holistic framework that utilises data analytics to examine threats to National Security has been exposed, which considers three main components, namely the Detonating Event, the Warning Period, and the Crisis Interpretation stage (see Figure 5.1).

As part of the Crisis Interpretation stage, this chapter presents a fine-grained methodology for the analysis of one Hybrid Tool (Social Media) to spot Hybrid Threats which are represented as the imbalance of the human security components,

and therefore extract, detect and interpret a variety of radical behavioural traits for National Security, by considering five steps namely Instability Scenarios, Entity Extraction, Wordlists Creation, Content Analytics, and Data Interpretation.

5.2 Hybrid Threats and Tools

Technology has placed the information environment into a dynamic arena where a set of heterogeneous actors tend to convey their ideologies and messages by using a combination of platforms to communicate an overall story or event. Within those actors, there might be citizens and non-state entities [96], who pursue their own interests and agendas, and in an unregulated virtual environment can lead to misinformation/disinformation [94]; resulting in the destabilisation of National Security.

Therefore, disinformation can be used as a strategy by the disruptive actors to mould people's behaviour using a mixture of real and digital world activities - hybrid threats [97]. The impact of these threats can be measured and applied to realworld scenarios by employing conventional and unconventional disruptive methods, spanning diplomatic, economic or technological contexts [93]. Hence, specific objectives/targets at a precise time [91] can be achieved, ranging from affecting critical infrastructures to creating confusion in order to strike the decision-making process of the state [93].

Hybrid threats are an integral part of modern conflicts/events leveraging disruptive tools to fuel such incidents. These tools or instruments of power, also called hybrid tools [91], contribute to intensifying the impact of the incident and can adopt a wide range of forms such as Propaganda, Domestic Media Outlets, Social Media, Funding of Organisations, or Strategic Leaks [91].

In this chapter, one Social Media instrument (the microblog Twitter) will be used to analyse different incidents aimed to detect and interpret radical behaviour that might affect National Security.

5.3 Detecting Hybrid Threats and Radical Behaviour (RQ4)

In all countries, managing national security is dealing with different challenges on a daily basis. Hybrid threats in itself is a complex challenges as they use multiple means tailored to take advantage of the vulnerabilities that society is facing [81]. The multi-faceted approach is what makes these kinds of threats difficult to detect [98].

According to [81] one way to detect a Hybrid Threat is by analysing the Political, Military, Economic, Social, Information and Infrastructure (PMESII) domains, which are closely related to the human security components proposed by [7] (Economic Security, Food Security, Health Security, Environmental Security, Personal Security, Communal Security and Political Security). Therefore one relevant component stakeholders might want to find answers to based on insights from data analysis is:

Q1. What sort of instability is the state dealing with based on the human security spectrum?

Social instabilities generate an environment where information can be used to undermine the confidence in the government, and therefore, the crisis can evolve until it affects the stability of the whole state. Cyberspace contributes to this complex scenario where individuals can create throw-away accounts to send their messages, taking advantage of apparent anonymity, the spread aggressive, violent and illegal viewpoints [99].

Calls of violence and violent views are a clear example of such behavioural patterns, where individuals try to influence social discourse through a variety of communication channels. Within the process of exchanging information via the Internet, the digital messages might nuance a set of different activities ranging from cyberbullying/victimisation, harassment, cyber-stalking, gang violence [100], to radical expressions [101].

According to [101], a radical expression refers to an act linked to a violent reaction, and such demeanour can be understood by analysing two "behavioural markers" proposed by [58] namely Fixation and Leakage. The former concept (Fixation)

refers to the trend to repeat constantly in a written message to a specific key term; whereas the second concept (Leakage) appertains to the intent to damage a particular target.

Both behavioural markers, Fixation and Leakage, need to spot the target that might be affected, which is why unveiling the associated entities/actors can provide more information about the incident. In this chapter, three actors/entities are proposed as critical players because of their importance for National Security.

- Location; As described in [83] [84] settlements can be structured hierarchically according to their shape and population numbers, namely Conurbation, Metropolis, City, Large town, Small town, Large Village, Small Village, Hamlet and Isolated dwelling. A crisis event can emerge at several locations within the same country. Hence, a two-pronged strategy as described by [82] can be used to cluster such incidents, to wit: City-Level and Widespread events.

- People; For this paper, only those political leaders whose unexpected absence due to an attack or any other disruptive event and that might trigger a state of instability, such as President, Head of state, Prime Minister or Vice president, etc., will be considered.

- Strategic Facilities; Threats to National Security such as terrorism, tend to affect the national infrastructure and the balance of security and liberty of a state, as described in [102]. One way to deal with such disruptive events is by analysing those messages regarding strategic facilities such as airports, means of transport, schools, universities, roads or hospitals.

Hence, four questions pertinent to the above elements are:

Q2. Which entities are being mentioned during a disruptive incident?

Q3. Which entities can be affected due to their proximity to the affected entity?

Q4. What are the intentions that individuals express around the affected entities?

Q5. Has the incident disseminated at several locations?

Furthermore, the aforementioned behavioural markers consider violence as a critical element, as a disruptive incident has unfolded. However, the term violence can adopt multifarious definitions according to the context that is being analysed. Such consideration brings the chance to address violence from dissimilar perspectives that range from killing, doing harm [100], or rioting and looting [103], activities that identify a conflict. Therefore, it becomes necessary to analyse violence expressions within social media messages to disclose the different nuances of violence, which is why the classification proposed by [82] will be used, as it describes a set of phrases that can be found when analysing disruptive incidents.

In view of these performative acts that can be found during a crisis, two more questions that need to be addressed are:

Q6. Have people conveyed violent expressions during the crisis?

Q7. Which kind of violent expressions is being posted by individuals during the incident?

Moreover, as described in Chapter 3 [67], *Coordination and Cooperation* is a stage part of the crisis interpretation process that refer to a cooperative system where individuals express actions during a disruptive incident aimed at reporting their needs that range from basic things such as water or shelter to objects that might comprise bombs, explosives or grenades. Hence, an additional question that needs to be addressed is:

Q8. Which type of necessities do people share on social media while a disruptive incident is taking place?

5.4 System Architecture

The methodological approach is shown in Figure 5.2, and it comprises five stages (Instability Scenarios, Entity Extraction, Wordlist Creation, Content Analytics, and Data Interpretation) which are aimed at detecting and interpreting radical behavioural traits through the analysis of one hybrid tool (Social Media).

The foundations of the process are based on the analysis of different societal elements as described in Section 5.3, which, in summary, enable to address eight questions that open up a multidimensional perspective since they provide key insights that can be used to interpret an incident.

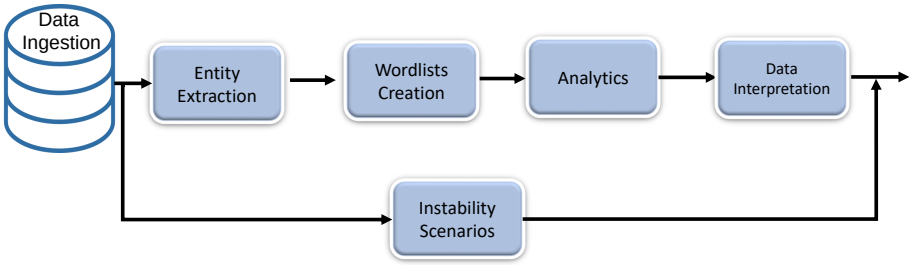


Figure 5.2: Proposed System Architecture

5.4.1 Instability Scenarios (Q1)

A crisis event is an unstable situation that undermines the societal structure of a state and may lead to a disaster [2]. As described in Section 5.3 an instability tends to expose the vulnerabilities of the state. Therefore the analysis of the human security aspects over time can become a critical factor since a peaceful social movement can quickly escalate into a violent riot.

As a result, the projection of different scenarios that reveal which human security components have been compromised and that can be seen as a vulnerability by others will enable to understand the sort of instability the society is facing.

In line with this idea, as described in Chapter 4 [89] a Deep Learning model was used to correlate the human security components, and the results suggested that individuals were involved towards a National Security issue when negative posts that involved Defence, Health and Government have been disseminated over the Internet.

These three variables (Defence, Health and Government) can be used to create four different scenarios, as shown in Figure 5.3.

Each scenario illustrates which human security components are being affected, but the proposed levels do not follow a hierarchical structure since National Security

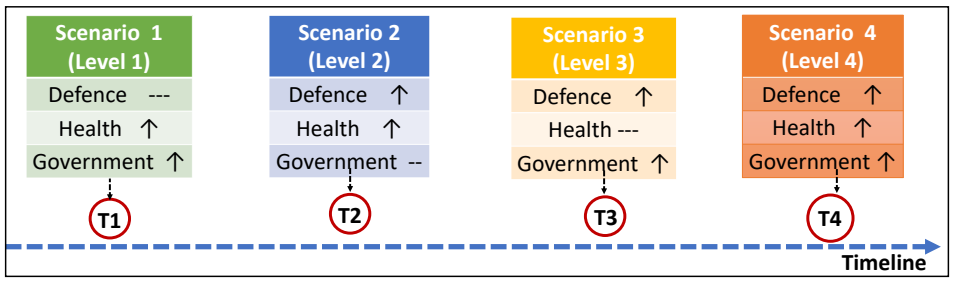


Figure 5.3: Illustration of the proposed National Security scenarios. Scenario 1 illustrates that Health and Government have been affected in T1. Scenario 2 indicates that Defence and Health have been compromised in T2. Scenario 3 shows that Defence and Government have been put out of balance in T3. Scenario 4 depicts that Defence, Health and Government have been affected in T4.

aspects are weighted in a dissimilar way from country to country.

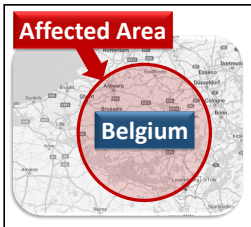
5.4.2 Entity Extraction (Q2 and Q3)

Entities are text expressions that contain special meaning such as names of people, locations or organisations [104]; however, data which flows within Social Media platforms present typographical mistakes since individuals tend to write their messages with a lack of capitalisation or by using short words to refer people's names, which in summary hinders the extraction of such terms.

Extracting such entities implies a complex process that requires as a first step to mine all major targets from the area where the disturbing incident is taking place (Knowledge Base Extraction). As described in Section 5.3, there are three main actors/entities that play the core role from a National Security perspective, namely Locations, People and Strategic Facilities.

For the purpose of this work, the knowledge base Wikidata was used to extract all the forenamed actors related to the critical area. These included airports, universities, gas stations, power stations (Strategic Facilities), villages, human settlements, counties, towns, highways, streets (Locations) and heads of state (People), see Figure 5.4.

As a second step (Token Replacement) tweets are tokenised and classified ac-



Towns	Airports	Streets
Neufchâteau	Ursel Airbase	Kemelstraat
Bastogne	Grimbergen Airfield	Hoogste van Brugge
Florenville	Namur-Suarlee Airport	Katelijnestraat
Messancy	Airport Asch	Stijn Streuvelsstraat
Hotton	Ursel Airbase	Sint-Jan in de Meers

Figure 5.4: Example of Location Extraction by querying the Wikidata Knowledge Base.

cording to the universal parts of speech code, as described in [105]. Then nouns are extracted because a typographic error can create confusion between an entity and a noun, and as described by [2] such grammatical errors downgrade the effectiveness of the conventional Named Entity Recognition techniques.

The third step (Semantic Matching) lies in performing a semantic match between the nouns extracted in the previous step (Token Replacement) against the entities extracted during the first process (Knowledge Base Extraction), in order to identify which entities are present in the analysed dataset (tweets). This process can be performed by considering a string matching process where words are index by sound, in this case, a phonetic algorithm such as SoundEx was selected because it encodes words and characters by analysing their sound or pronunciation as described in [106], and in this way spelling errors can be detected.

However, one issue is that nouns are unigrams and entities (locations, people or facilities) are phrases that can act as single words (collocations) such as New York or Hong Kong. Hence, those entities that acted as collocations were joined as single words by using an underscore (new york –> `new_york`), then these set of new words were replaced in the original dataset (tweets), and afterwards, the Token Replacement and Semantic Matching processes were performed again. This step is crucial because, in such a way, nouns can represent either a word just as capitol or a complex phrase such as `hong_kong`.

The resulted nouns can be enriched or expanded. It was an enriched noun when collocations were corrected, whereas the noun was expanded when the word is an acronym, and it takes its original form, as shown in Table 5.1.

Table 5.1: Example of Enriched and Expanded nouns

Nouns	Enriched Noun	Expanded Noun	Wikidata Description
new york	new_york	-	Global City
mong kok	mong_kok	-	Human Settlement
un	-	united_nations_organisation	International Organization
nato	-	north_atlantic_treaty_organisation	Military Alliance

According to [107] *Critical National Infrastructure* refers to those elements of infrastructure, which in case of being lost or compromised can impact on national security. In line with this idea, critical elements can be extracted by considering its proximity to the entities that have been identified from the previous step (Semantic Matching), such process can be performed by mining the information from a knowledge base such as Wikidata (see Figure 5.4).

Finally, all nouns that were recognised as entities have to be labelled by tags according to the knowledge base description (see Table 5.1).

5.4.3 Wordlists Creation

As described in Section 5.3, radical activity is linked to various violence nuances; however, detecting such behavioural patterns within social media messages represents a challenging task.

One way to deal with such a task is by creating a set of wordlists that contain nouns and verbs that enable the identification of specific actions and particular objects, such as weapons or means of transport. Therefore, this process can be dissected into three areas. The first area is focused on spotting those actions that reveal violent or non-violent actions; which is why the classification proposed by [82] can be used as a template to create the first dictionary (Dictionary of violence terms) which contains verbs and nouns related to both harsh and non-harsh activities.

The second area is aimed to create a dictionary (Dictionary of nouns) that classifies nouns/objects by its nature; for this work, seven different clusters were created, namely communication routes, people, songs, supplies, vehicles, weapons and types

of waste. This dictionary is a core asset since it specifies whether the noun is a mean of transport, an explosive or a person (see Table 5.2).

Table 5.2: Object classification dictionary

Noun Classification	Description		
Communication Routes	Road	Street	Thoroughfare
People	Protestor	Police	Soldier
Weapons	Teargas	Bullet	Dynamite
Supplies	Food	Water	Bread
Songs	Anthem	Song	Lyric
Vehicles	Car	Bike	Scooter
Types of Waste	Rubbish	Excrement	Trash

The last area is centred on creating a dictionary (Dictionary of verbs) which includes a list of verbs that describe a large group of activities; this is a key component because a range of intentions can be detected and in such a way policymakers can understand what sort of purposes people are conveying, such as occupy, assassinate, block or say, as shown in Table 5.3.

5.4.4 Analytics (Q4 to Q8)

The interpretation of an incident needs the characterisation of reality which is a reflection of social behaviour, but measuring social perception requires the understanding of the set of actions performed by others, as described in [108]. Therefore actions can be described by verbs, which is why the interpretation process utilises verbs and nouns as the bedrock of this analysis.

In the first instance, this study considers the sentence breakdown where the basic parts are the subject, the verb and the object. Hence, the direct object is a noun phrase that expresses that an object/person is the recipient of an action verb.

Figure 5.5 depicts clear examples of noun phrases, where verbs express the intentions/actions, and the nouns represent the objects being acted upon. As a result,

Table 5.3: Example of verbs that can be used to interpret actions. Adapted from [60]

Verb Classification	Description		
Build Verbs	Build	Arrange	Churn
Verbs of Change of State	Crash	Break	Shatter
Verbs of Communication	Explain	Say	Convey
Verbs of Contact by Impact	Bang	Beat	Strike
Fill Verbs	Block	Bombard	Flood
Want Verbs	Need	Want	Hope
Future Having	Feed	Give	Donate
Verbs of Psychological State	Affect	Arouse	Agitate
Verbs of Social Interaction	Argue	Combat	Clash
Verbs of Creation	Build	Assemble	Bake
Verbs of Killing	Eliminate	Immolate	Liquidate

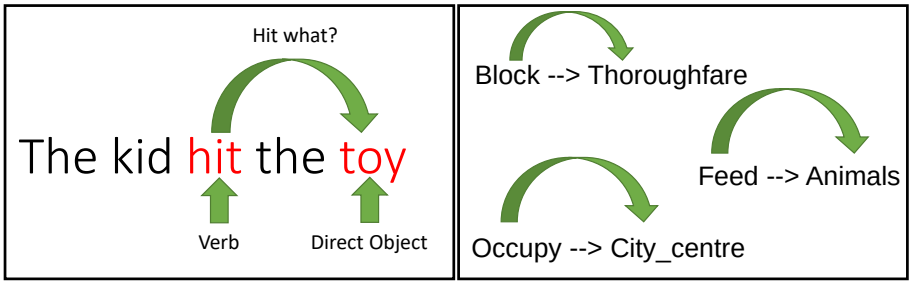


Figure 5.5: Direct object sample

the direct object can be used to create a high-level summary of the analysed corpus. In a similar fashion to Chapter 5 and described in [109], noun phrases are extracted, but in this case verbs are classified according to the dictionary of violence terms and the dictionary of verbs described above, and as far as nouns are concerned, they are categorised according to the entities and the dictionary of nouns previously mentioned.

In addition to the aforementioned method, a different technique can be used to enrich results such as word embeddings. This technique was selected because of its powerful way to represent words as vectors. This is important as word vectors can show the semantic relationship between words [110]. However, when analysing radical events, scenarios are complex and varied since the necessities and targets that individuals pursue are different, which is why the semantic relationships between words will vary as well, and events need to be evaluated separately.

For this work, the GloVe model was selected because it is an unsupervised learning algorithm focused on obtaining vector representations for words, as described in [111]. The GloVe model was trained by using the skip-gram method because the context in which words appear is a crucial factor, and in order to improve the quality of results a list of stopwords was removed from the datasets to create the vocabulary, and verbs were lemmatised.

Finally, examining the terms from the GloVe model was addressed in two ways. Firstly, verbs from the dictionary of verbs previously mentioned were used to find which word/noun reflect a semantic relationship, based on the specific context. Secondly, the verb and the direct object from the previous process were used to perform a mathematical operation (addition) between them, since those set of words can be considered as vectors, see Figure 5.6.

5.4.5 Data Interpretation

Interpreting data requires to organise the information in a specific manner that make it understandable. In line with this idea, the GloVe and direct object processes issued noun phrases that are formed essentially by two main elements, namely a verb and a noun. As explained in Section 5.3, verbs denote performing an activity/action

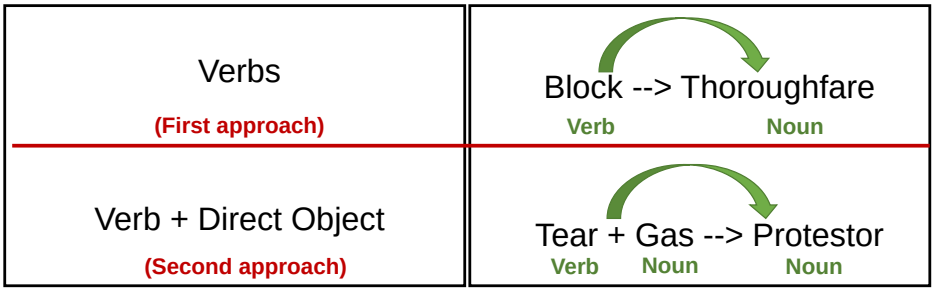


Figure 5.6: Examining terms in the GloVe model to detect Radical Behavioural traits

but classifying such set of activities according to its meaning is a challenging task, which is why the categorisation proposed by [60] opens up a broad perspective.

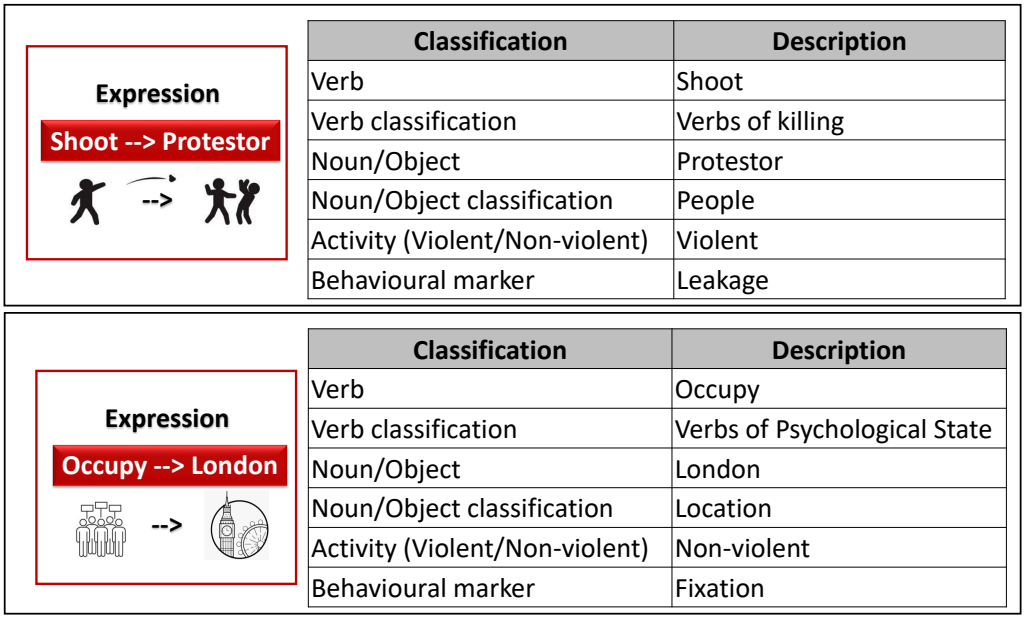


Figure 5.7: Interpretation process example

Therefore, actions can be divided into eleven groups, as depicted in Table 5.3, where activities such as kill, assassinate or block can disclose a manifest intention.

By contrast, nouns adopt different roles such as people, an object or a location; but by linking verbs that reveal a violent action with such nouns, new insights come to light and unveil radical behavioural traits and violent activity, see Figure 5.7.

Regarding the coordination and cooperation traits, verbs that reflect the transfer of property will provide the evidence that people are looking for items or are

offering them (e.g. bring pistol or need grenade). Such a list of verbs are based on the classification proposed by [60] and for this work verbs of creation, verbs of communication and future having will be considered to create the correspondent lexicon.

5.5 Experiments and Validation

To demonstrate the validity and the robustness of the proposed methodological approach (see Figure 5.2), real disruptive incidents have been examined. The micro-blogging data from the protests in Hong Kong and the Ferguson riots in the United States of America described in Chapters 4 and 5 have been used for validation purposes.

As portrayed earlier, both events were polarised by negative sentiments, but in this case, the extraction of radical behavioural insights is the aim of the present analysis. As a preliminary step, the data corpora were cleansed and processed similarly to Chapters 4 and 5, and as explained in [89, 109].

5.5.1 Instability Scenarios (Q1)

When facing a crisis event, one question that must be answered is: What sort of instability is the state dealing with based on human security spectrum?

In order to tackle the former problem, tweets were classified into the ten aspects of human security components, as described in [7], to wit: Economy, Defence, Environment, Government, Health, Information, Life, Transport, People and Public Order.

This process was performed firstly by producing word embeddings to learn the context, and secondly, the embeddings were classified using a machine learning model. In this work, the word2vec algorithm was selected in view of its power to associate a vector with a word [110] [112], and a popular technique to categorise them - Gradient Boosting Machine-.

As time is a core factor in understanding the evolution of an incident, the percentage of each human security component was calculated per day, then to create

the instability scenarios only three components were considered (Defence, Health and Government), as mentioned in Subsection 5.4.1.

1. **The Hong Kong Protests**:

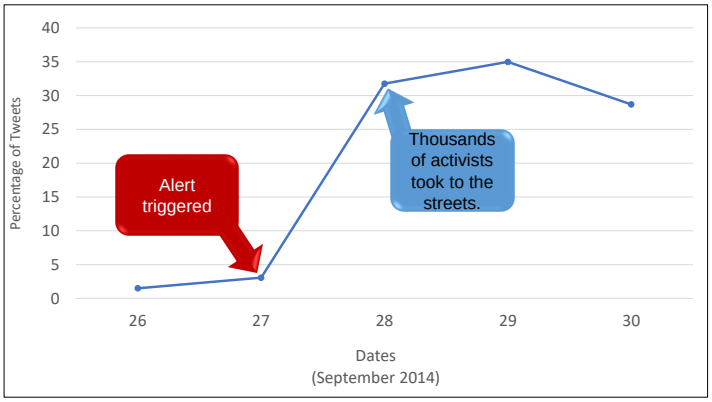
   This event described a series of protests in 2014 when people began to manifest their discontent after a decision regarding the Hong Kongese electoral system was issued. The analysed period extends from September 26th —30th, 2014 as depicted in Figure 5.8.I.

   For this case, Figure 5.9 illustrates that on the date the system spotted the tipping point (September 27th), the affected human security components were Defence and Government. During the next two days (September 28th-29th), when protestors took the streets, the components changed to Health and Government, which suggests that people's health was compromised. The incident escalated a day after (September 30th) since three components were affected: Defence, Health, and Government.

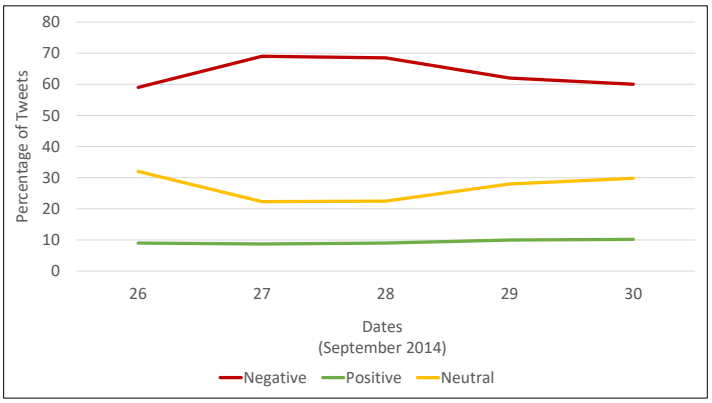
2. **The Ferguson Riots**:

   These protests and riots began after the fatal shooting of a man by a police officer in 2014. The analysed period was from November 11th to 30th, as shown in Figure 5.8.III.

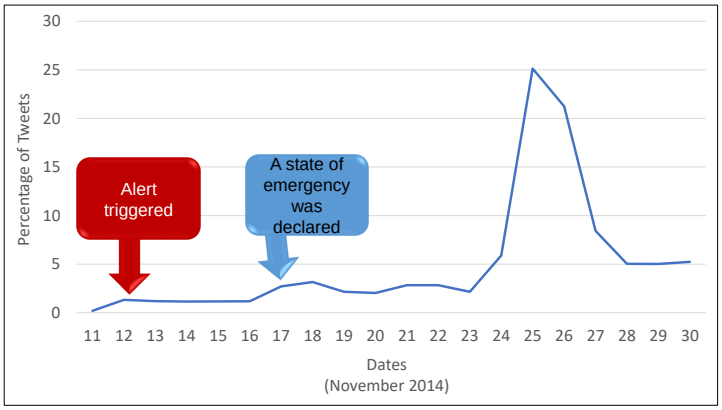
   As displayed in Figure 5.10, the date where the tipping point was detected (November 12th), two human security components were disturbed, namely Health and Government. The following two days, the scenario changed as three components showed disturbance (Defence, Health and Government), which suggests that societal problems escalated. A day before the governor declared an emergency estate (November 16th), the same scenario of three affected variables showed up.



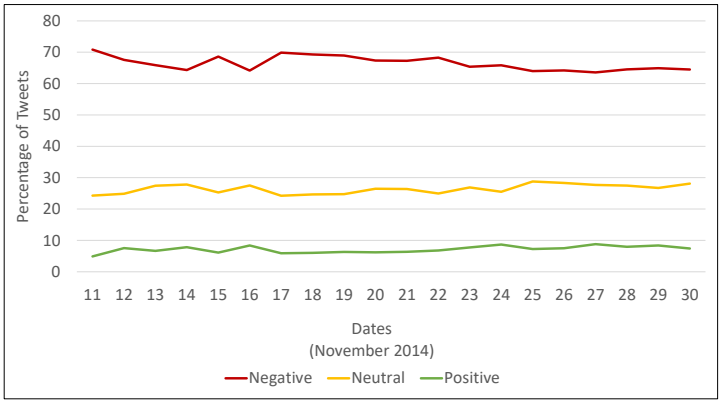
I. Tweets from the Hong Kong protests



II. Sentiment Analysis of the Hong Kong protests



III. Tweets from the Ferguson riots



IV. Sentiment Analysis of the Ferguson riots

Figure 5.8: Timeline of protests and Sentiment Analysis

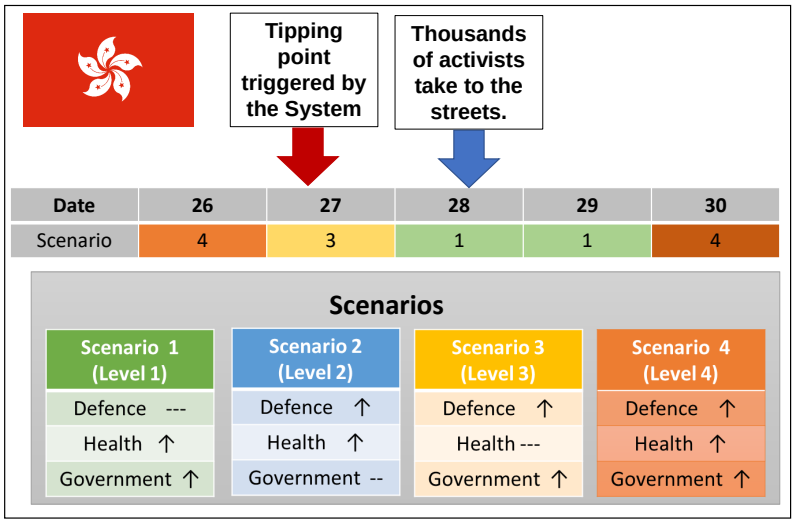


Figure 5.9: Instability Scenarios in Hong Kong

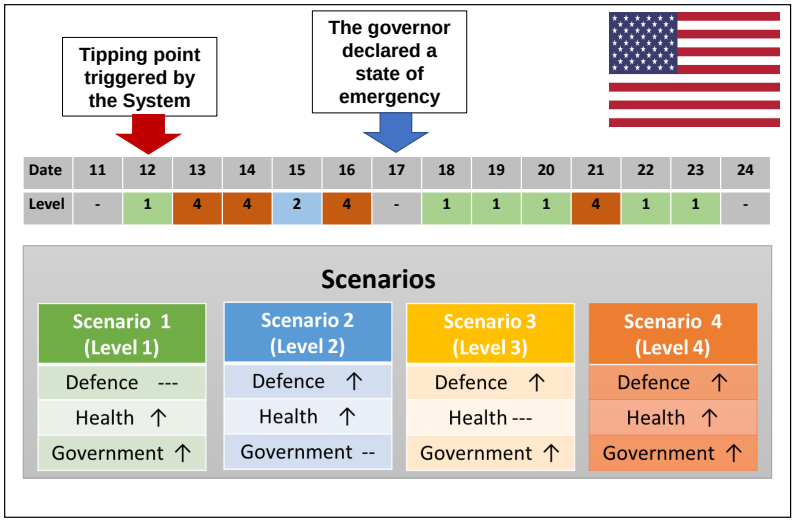


Figure 5.10: Instability Scenarios in the USA (Ferguson riots)

5.5.2 Entity Extraction (Q2 and Q3)

After analysing instability scenarios over time, the next stage involves the extraction of main entities. This process represents a core stage because it enables identifying people, locations, and strategic facilities that can be considered vital targets, as described in Section 5.4. Therefore, the entity extraction process was performed by considering a daily time frame, following the architecture depicted in Figure 5.2 described above.

1. **The Hong Kong Protests**:

Q2. During this process, fifty-five entities were extracted, but for visualisation purposes, Figure 5.11 shows their distribution over time. These results suggest that on September 27th (Tipping point), individuals posted messages related to cities, human settlements, neighbourhoods and a human being - President of the People's Republic of China-. This last entity might explain why the human security component -Government- is present in Scenarios 4 and 3, as shown in Figure 5.9.

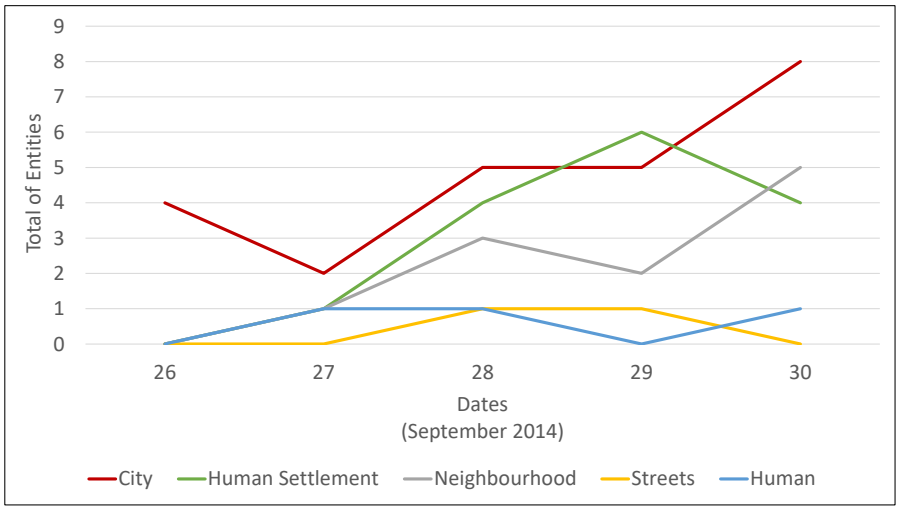


Figure 5.11: Distribution of extracted entities (city, human settlement, neighbourhood, street and human) during the Hong Kong protests over time

A day after the tipping point was detected, individuals began sending messages about specific locations such as streets, and an activity ramp-up in entities

such as cities, human settlements and neighbourhoods, which suggests that the incident was spread between different places.

Q3. Based on the entities extracted from the previous step, strategic targets were mined according to its proximity by considering the criteria proposed in Section 5.4. For exemplifying the results, entities that were close (2 Km) to one of the extracted entities are shown in Figure 5.12.

Entity (Human Settlement)	Streets within 2 Km
	• Shanghai_Street
	• Kowloon_park_drive
	• Ashley_road
	• Li_sing_street

Figure 5.12: Example of strategic entities close to the affected area (Mong Kok)

2. **The Ferguson Riots**:

Q2. In this case, four entities were mentioned constantly over time, namely Ferguson (town), Florissant (City), `Hereford_avenue` (road) and `Jay_nixon` (human being).

Q3. By considering Ferguson (town) as the axis of analysis, Figure 5.13 depicts some strategic facilities that can be extracted by considering a distance of 5 to 10 km from this location. It should be noted that these targets can provide a holistic view to deciding which entities need to be protected.

5.5.3 Analytics and Data Interpretation (Q4 to Q8)

As described in Section 5.4, a high-level summary is required to analyse, interpret and detect radical behavioural traits for National Security, so two different techniques were used to address that task, namely direct object and word embeddings.

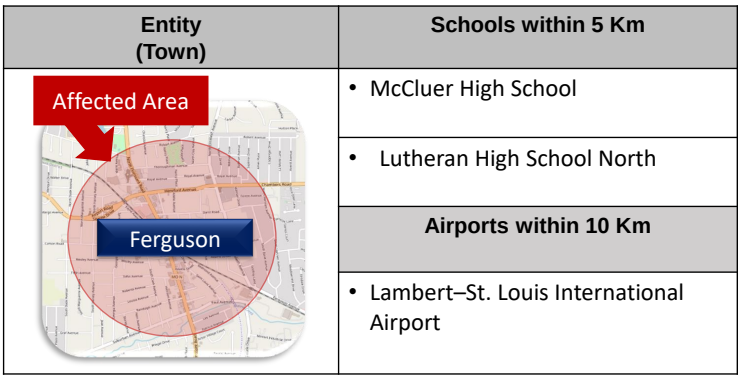


Figure 5.13: Example of strategic entities close to the affected area (Ferguson)

1. **The Hong Kong Protests**:

Q4. Table 5.4.II depicts that the word embeddings process detected that individuals expressed their intention to occupy Central (neighbourhood) just a day before the system spotted the tipping point. By contrast, the direct object process (see Table 5.4.I) identified that activists conveyed the intent to occupy Wanchai (neighbourhood), Mong Kok (human settlement) and Hong Kong (city) just the date when thousands of people took the streets.

Q5. Since individuals expressed their purpose to occupy multiple locations, this result suggests that the incident can be classified as a widespread event.

Q6. As described in Section 5.4, the dictionary of violence terms contains verbs and nouns related to violent activities. As a result, the word embeddings process spotted turbulent activity when the tipping point was triggered because people described that they were suffering a tear gas attack and on subsequent days such violent activities continued as people conveyed gas attack, tear gas bullets and tear gas fire. On the other hand, the direct object process identified violent acts as well, by the date when the streets were taken, as messages related to throwing canisters, clashing protestor, or a tear gas attack was published. It should be noted that messages regarding setting barricades, assembling barricades or occupying swaths were conveyed, although such activities are not considered as violent according to the classification proposed by [82], they can contribute to creating a plan for deciding the best course of action.

Q7. In this case, expressions linked to suffering a tear gas attack and throwing objects (canisters) are the violent expressions conveyed by individuals.

Q8. The Hong Kong case reflects that people sent tweets that denote the necessity of food, especially to donate noodle (September 30th).

Table 5.4: Extraction of radical behavioural expressions using direct object dependencies and word embeddings during the protests in Hong Kong (September 2014).

Date 26	**Date 27**	**Date 28**	**Date 29**	**Date 30**
show =>solidarity	leave =>Hong Kong	occupy =>Wan Chai	occupy =>Mong Kok	occupy =>Mong Kok
	set =>barricade	occupy =>Mong Kok	visit =>Mong Kok	take =>admiralty
	kick =>blockade	occupy =>Hong Kong	tame =>Wanchai	**donate =>noodle**
		spread =>Mong Kok	protest =>Hong Kong	extend =>disobedience
		build =>barricade	occupy =>hongkong	keep =>sausage
		break =>blockage	shut =>barricade	hit =>admiralty
		threaten =>protester	disturb =>explode	set =>barricade
		throw =>canister	set =>barricade	
		get =>injure	disrupt =>protester	
		cut =>comms	clash =>protester	
		occupy =>swath	cover =>barricade	
		assemble =>barricade	disrupt =>spree	
		set =>roadblock		
		tear =>demonstrator		

I. Direct Object

Date 26	**Date 27**	**Date 28**	**Date 29**	**Date 30**
occupy =>Central	tear =>gas	tear + gas = fire	take =>street	shake =>retweets
boycott =>class	chant =>crowd	occupy =>Central	tear +gas = fire	tear + gas = use
break =>civic		bullet + Rubber = Violence	burn =>violence	show =>drone
take =>fight		hit =>demonstration	call =>democracy	massacre =>Tiananmen
email =>disobedience			attack =>spray	teargas =>bullet
			block =>Instagram	threat =>death
				bullet =>teargas
				attack =>police

II. Word Embeddings

2. **The Ferguson Riots**:

Q4. Table 5.5 displays that the direct object process detected on November 12th

(tipping point), individuals manifested their intentions to occupy Ferguson (town).

Q5. According to the analysed data corpus, individuals expressed the purpose to occupy one location, which is why it can be considered as a city-level event.

Q6. The Ferguson case shows that both processes, the direct object and word embeddings, disclose violent activity when the tipping point was triggered, as actions such as organising riot, organising boycott, looting, stealing or burning were posted, and that kind of activity persisted during the following days, but also adding actions such as throwing excrement, throwing grenades or throwing dynamite (see Table 5.5).

Q7. For this case, expressions linked to shooting protester or shooting thug was expressed before the tipping point, but a day after expressions such as shooting policeman or shooting black people were conveyed.

Q8. This particular event unveils a violent nature, but expressions such as offering dynamite, buying a weapon, buying ammunition, needing grenades, bringing grenades or building IED (improvised explosive device), suggests that social media worked as a mean to weaponise the incident.

5.6 Conclusion

This chapter has introduced a novel technical methodology to analyse, detect and interpret radical behavioural traits by considering five steps, namely Instability Scenarios, Entity Extraction, Wordlists Creation, Analytics and Data Interpretation.

The proposed methodology enables a holistic analysis of the incident by:

- Creating scenarios to identify changes in human security components and,
- Extracting core entities relevant to the incident. These entities include:
  (a) Locations
  (b) People

(c) Strategic facilities (determining dissemination at several locations) and,

(d) Those affected because of their proximity to the incident.

In addition, such analysis is complemented by detecting violent and non-violent expressions, and those instruments that can be used during the crisis, which can affect or complicate the way the event is evolving.

The validity and robustness of the proposed methodology have been demonstrated in the interpretation of radical behaviour during the protests in Hong Kong and the Ferguson riots in the USA. Results showed that violent expressions are different according to the nature of the incident and particular context.

Table 5.5: Extraction of radical behavioural expressions using direct object dependencies and word embeddings during the protests in Ferguson (November 2014).

Date 11	Date 12	Date 13	Date 14
Organize =>Boycott	Set =>Barricade	Shoot =>Policeman	Shoot =>Looter
Organize – Riot	Shoot =>- Thug	Put =>- Curfew	Throw =>- Canister
Shoot =>- Riot	Bring =>Grenade	Shoot =>Protester	Shoot =>Protester
Prepare =>Riot	Occupy =>Ferguson	Need =>Grenade	Need =>Grenade
Shoot =>Protester	Stop =>Looter	Buy =>Grenade	Give =>Molotov
Loot =>Commit	Burn =>- Loot	Get =>Weaponry	Loot =>Kill
Loot =>Ferguson	Loot =>- disperse	Sell =>Pistol	Shoot =>Looter
Steal =>Loot	Get =>Loot	Loot =>Rise	Loot =>Zionist
		Loot – Steal	Loot =>Pillage
		Burn =>- Loot	Buy =>Pistol
		Loot =>- Arm	
		Stop =>Loot	
		Loot =>- Attack	
		Loot =>Ferguson	

Date 15	Date 16	Date 16
Throw – Canister	Throw =>Poop	Throw =>Poop
Shoot =>Nigga	Shoot =>Teenager	Shoot =>Teenager
Shoot =>Looter	Shoot =>Thief	Shoot =>Thief
Loot =>Riot	Shoot =>- whitehead	Shoot =>- whitehead
Loot =>Kill	Steal – Loot	Steal – Loot

I. Direct Object

Date 17	Date 18	Date 19	Date 20
	Shoot =>Feral	Shoot =>- Niggas	Shoot =>Protester
Buy =>Ammunition	Buy =>Ammunition	Shoot=>Teenager	Move =>weaponry
Shoot =>Protestor	Throw- Canister	Loot =>Ferguson	Shoot =>Niggas
Shoot =>Negro	Buy =>Weaponry		Loot =>Commit
Shoot =>Looter	Loot =>riot		
Loot =>Fight	Loot =>Shoot		
Loot =>Steal	Loot =>- Missouri		
Loot =>Ferguson	Loot =>Protester		
	Loot =>Ferguson		

Date 21	Date 22	Date 23
Shoot =>Protester	Offer =>Dynamite	Throw =>Dynamite
Tear =>Barricade	Build =>- IED (improvised explosive device)	Throw =>Grenade
Loot =>Riot	Set =>Barricade	Set =>Barricade
	Push =>Barricade	
	Loot =>Protester	
	Loot =>- Ignite	

II. Word Embeddings

Chapter 6

Ideology

6.1 Introduction

Civil unrests, rioting and protests are events generated by a myriad of factors including violence against minorities, economic issues, social problems or political-related incidents, and the aftermath of such disruptive episodes may carry adverse effects such as boycotts or other long-term consequences that may create instability in a state [113]. However, understanding the ideas which are behind the scenes, may disclose prevailing ideologies that are shaded by emotional states ranging from anger, disgust, sadness, surprise, fear, trust, and joy to anticipation [63], (see Figure 6.1).

In connection with such emotional states, public demonstrations manifest negative perceptions regarding the objects of emotion, namely the opponent and the contentious issue, as described by [114]. Therefore, the aforementioned aspects play a significant role as they contribute to justify intergroup violence such as politically motivated events, which can be nuanced as violent street rioting or attacks targeted to specific groups [115]. As a result, amidst an incident, violence becomes a core feature that contributes to analysing a variety of situations, such as discontent or deprivation, and where such factors can work as a seedbed of events linked to radical activity [116].

Due to adverse effects, violent-related activity is not socially accepted [116], which is why it requires ideological support to understand it [115]. In line with this idea, ideology refers to social representations shared by groups of people which rep-

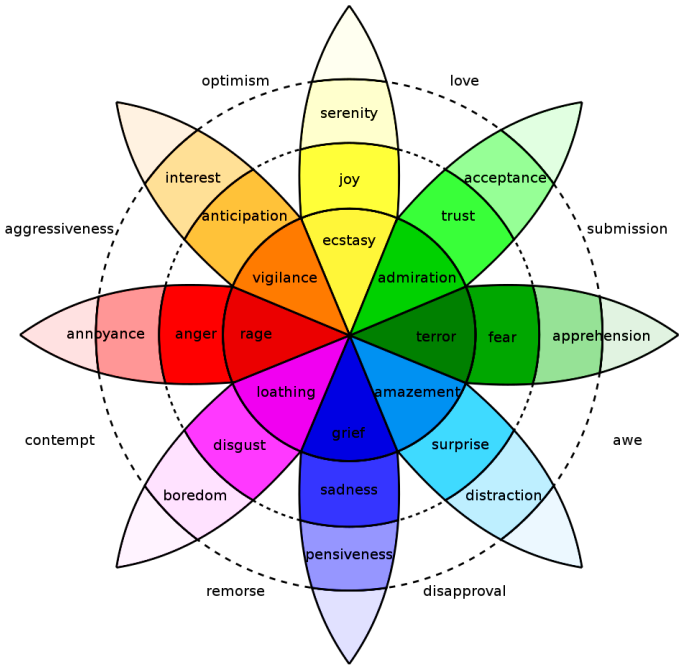


Figure 6.1: Plutchick's wheel of emotions, adapted from [63].

resent their essential interests or beliefs, and at the same time, ideology gains a core role when situations regarding competition, conflict or domination are present.The link amidst conflict and ideology become stronger when such groups of individuals are involved in disruptive events, as described by [117].

According to [118], a person who holds a hostile relationship towards an individual or group perceived as powerless is called authoritarian. Moreover, [119–122] describe that authoritarianism is closely associated with political ideology, where such a type of ideas/beliefs along with the encouragement of social control and security can lead to political violence against dissimilar groups of people, as described by [119].

As stated by [115] authoritarianism can be visualised as an ideological attitude, and it considers three main factors in agreement with [119], namely **aggression, submission** and **conventionalism**. Furthermore, such a type of ideology can estimate a wide range of attitudes such as anti-democracy, restriction of civil liberties, political intolerance or abusive behaviour, among others as suggested by [115].

Hostility, on the other hand, is a feeling directed on groups of individuals [123], and according to [124] reflects collective emotions that denote appraisals of superi-

ority/inferiority, injustices or intolerability, which can be seen whilst incidents take place. The interstitial relation of authoritarianism and hostility lies in the latter is an essential attribute that characterises the authoritarian personality [123]; furthermore, as described by [118], groups with higher authoritarianism traits have greater overt hostility than those groups with a lower tendency on such a trait.

Therefore, hostility in a similar fashion to authoritarianism can be dissected into different elements to appreciate it. As a result, [114,124] proposed three components, namely **anger, contempt** and **disgust**. What is more, the aforementioned triad can be seen as a unit that under stress conditions can trigger an explosive mixture of emotions leading to intergroup hostility, and political violence [124].

Based on the concepts delineated above, this chapter investigates data analytics approaches for analysing ideology. In particular, an ideological attitude, authoritarianism, and an attribute related to it, hostility, is examined using a variety of computational techniques. Firstly, an unsupervised learning technique (variational autoencoder) is used to train a model aimed at spotting the ideological features mentioned above. Secondly, polarisation analysis and natural language processing techniques, are implemented to extract useful information as entities and actions; and at the same time, identify violent and non-violent actions embedded in text labels (hashtags).

The methodology of this study was evaluated by examining one event linked to disruptive situations, namely the protests in Puerto Rico in 2019.

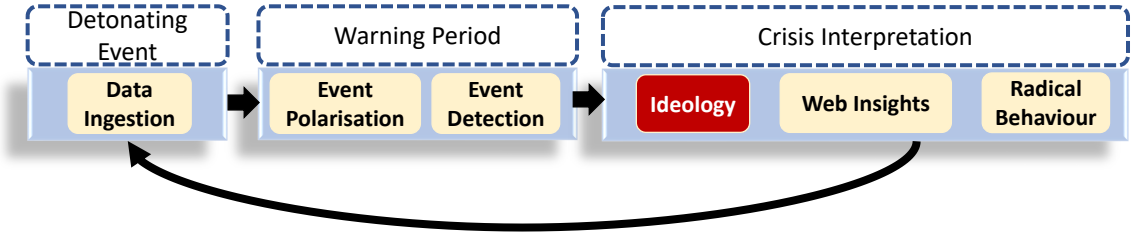


Figure 6.2: Conceptual Framework for Social Movements Analytics for National Security.

In addition and contextualising the ideology stage within the conceptual framework described in previous chapters (see Figure 6.2), this process contributes to

complete the crisis interpretation phase, which is focused on construing and extracting behavioural features by creating a big picture of the studied incident.

6.2 The importance of studying Ideology

As explained in [125] adopted ideas or beliefs tend to shape popular Ideology, and the analysis of this topic has conducted different research projects due to the dissimilar perspectives or paths such a theme can embrace. Indicative illustrations of some paths proposed to examine Ideology utilising data analytics are depicted in Table 6.1. A first approach described by [126] examined such a theme focusing on a hot-button topic as abortion. In this study, a triplet of categories was used to group ideas on abortion, namely for, against and neutral. Moreover, the authors used supervised learning models along with topic modelling techniques and linguistic characterisation to address the discourse across the aforementioned subject.

Table 6.1: Related works aimed at analysing ideology based on different perspectives.

Related work	Techniques	Data analysed	Objective
[126]	Unsupervised learning model and topic modelling.	Social media content (Twitter).	Analysing ideology form the perspective of abortion.
[127]	Network analysis and unsupervised learning model.	Social media content (Twitter) and surveys.	Estimating the individual-level of ideological position.
[128]	Web-graph analysis and regression models.	Textual information (online forums) and surveys.	Analysing online groups on opinion extremism.
[129]	Regression analysis.	Survey data.	Analysing factors linked to terrorism.
[130]	Sentiment Analysis.	Social media content (Twitter).	Analysing political discourse.

A second work was proposed by [127] who examined social media content to estimate individual-level ideological positions categorising them as political elites, parties or citizens. In such a study, two sources of data were used, tweets and information coming from a survey tool. Therefore, the resulting mixture of data was processed using unsupervised learning techniques and network analysis.

A different study focused on analysing radical and ideologically homogeneous online groups (extremism), using survey data and textual information extracted from online forums was suggested by [128]. In this work, web-graph analysis together

with regression models were the primary tools aimed at examining this type of behaviour. In connection with radical demeanour, the research discussed in [129] examined terrorist ideology through a survey and regression analysis to visualise the factors that contribute to potential terrorist actions.

The analysis of political discourse is a different way to analyse ideology, as explained by [130]. In this work, messages posted by political elites are examined to understand the way political ideologies are disseminated. For that purpose sentiment analysis was used.

The studies previously described are instances of how to examine Ideology by considering nuances as extremism, political aspects and ideological discourses. Data coming from surveys and social media content were used to feed these works together with different computational techniques to analyse the information. However, the novelty and contributions of this chapter to analysing Ideology in the context of national security are centred on four main aspects.

1. Ideology is analysed based on authoritarianism and its associated attribute, hostility. These factors enable to examine disruptive events in the context of of national security aspects.

2. An anomaly detection model is proposed, which is trained using other real incidents to calibrate the aforementioned ideological features, utilising an unsupervised deep learning generative model.

3. Polarisation analysis together with natural language processing is used to extract numerous entities (people, object, location and events) and actions (verbs), which contribute to identifying both violent and non-violent activities embedded in words or phrases such as hashtags.

4. The methodology is integrated as a critical stage within a holistic analysis framework, aimed at creating a big picture of the studied incident.

6.3 Dissection of Ideological elements

As described in Section 6.1, emotions play a central role during a protest since they represent an action or state of mind throughout a particular situation [131]. Moreover, studying ideology in the context of authoritarianism and hostility involves the analysis of emotions. Therefore, as outlined in [132] emotions are integrated by a set of basic emotions, namely anger, anticipation, disgust, joy, trust, fear, surprise and sadness (see Figure 6.1). What is more, every sentiment is integrated by adding the set of basic emotions, resulting in dyads [63]. Hence, as [63] theorised primary dyads are represented by the addition of two basic emotions as contempt= disgust + anger, by contrast, secondary dyads are formed by emotions which are two petals apart as envy= sadness + anger. The tertiary dyads are composed of emotions that are three petals apart, as shame= fear + disgust (see Figure 6.1).

As detailed in Section 6.1, [119] suggested that authoritarianism comprises three factors, namely aggression, submission and conventionalism. Furthermore, hostility is an emotional mixture of anger, contempt and disgust. Hence, following the emotion wheel outlined by [63], the components mentioned above (authoritarianism and hostility) were calculated as presented in Table 6.2.

Table 6.2: Dyads and emotions of authoritarianism and hostility, adapted from [63].

Authoritarianism		Hostility	
Description	Emotion/Dyad	Description	Emotion/Dyad
Submission =	Trust + Fear	Anger	Emotion
Aggressiveness=	Anticipation + Anger	Disgust	Emotion
Conventionalism =	Shame + Guilt	Contempt =	Anger + Disgust

6.4 Methodology to Analyse Ideology (RQ5)

The proposed approach for unveiling ideological features is illustrated in Figure 6.3. The complete process involves four stages, namely, Data Ingestion, Information Extraction, Training and Threshold Calculation and Hashtag Analysis. These stages are described in the following subsections.

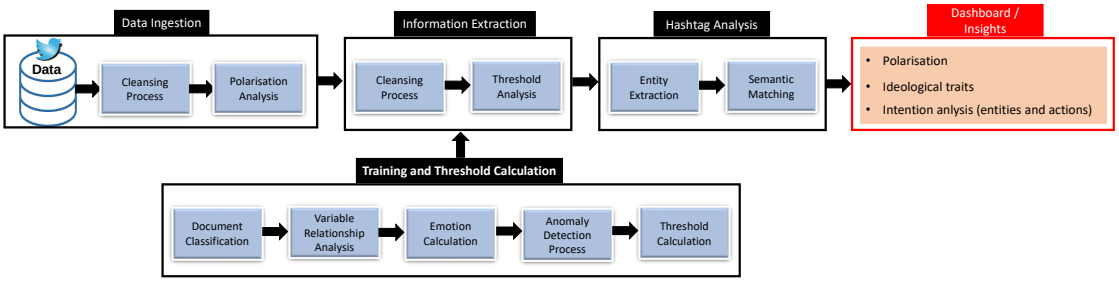


Figure 6.3: Proposed Methodology for Unveiling Ideological Features.

6.4.1 Data Ingestion

The data collection procedure represents the backbone of the entire process, as it provides the raw material the following steps will work with. Such a consideration require special attention while a crisis takes place due to the extensive amount of information that flows throughout social media forums [2]. Consequently, for the purpose of this chapter, Twitter was selected as the primary source of information because of its power to disseminate critical data along with the number of individuals that can be reached in a short time span.

In order to select useful information amidst the large volume of data that Twitter generates, hashtags regarding the spotted incident are selected, and afterwards, tweets linked to such hashtags are collected, then they are processed using the following two steps.

1. **Cleansing Process**:

   Firstly, URLs, RT and mention expressions are extracted. Secondly, contractions are replaced, such as isn't: is not. Thirdly, punctuation marks together

with stopwords are removed, and slang expressions are replaced by using complete terms based on a preconfigured wordlist, for instance: "FYI": For your information or "TBH": To be honest.

The importance of this process has two main paths. Firstly, slang expressions are language nuances that people tend to use to convey and stress their feelings positively or negatively, and in such a way, may affect the polarisation analysis process. Secondly, slang terms have different semantic forms which may vary from country to country, which is why the usage of a preconfigured dictionary can narrow down the analysis of these type of terms.

2. **Polarisation Analysis**:

   Analysing events require identifying the predominant sentiment conveyed by individuals. In the same vein of chapters, 4,5 and 6 and as detailed in [89, 109, 133] a sentiment analysis process is carried out, aimed at pinpointing the foremost polarisation (positive, negative or neutral) around the studied dataset.

6.4.2 Training and Threshold Calculation

Ideology studied in the light of authoritarianism and hostility can be appreciated in manifold degrees, depending on the context of a particular incident and in which way human security aspects are affected, namely economic security, food security, health security, environmental security, personal security, communal security and political security [7]. Therefore, examining dissimilar events enable a holistic view of how the aforementioned ideological traits might change.

The primary purpose of the training and threshold calculation procedure lies in setting thresholds for both authoritarianism and hostility traits, which will be used in Section 6.5 to examine a different nuanced incident. In connection with such an idea, two incidents were selected looking upon the different nature that triggered them, namely, the protests in Catalonia due to the referendum on independence in 2017 and the demonstrations at the border between Gaza and Israel because of the moving of the US embassy to Jerusalem in 2018. Hence, two sets of information

were created using the historical Twitter API and following the steps outlined in the Data Ingestion procedure. The collected data ranged from September 19th to October 5th, 2017, in the case of the Catalonian incident and May 8th-18th, 2018, for the conflict in Gaza (see Figures 6.4 and 6.5).

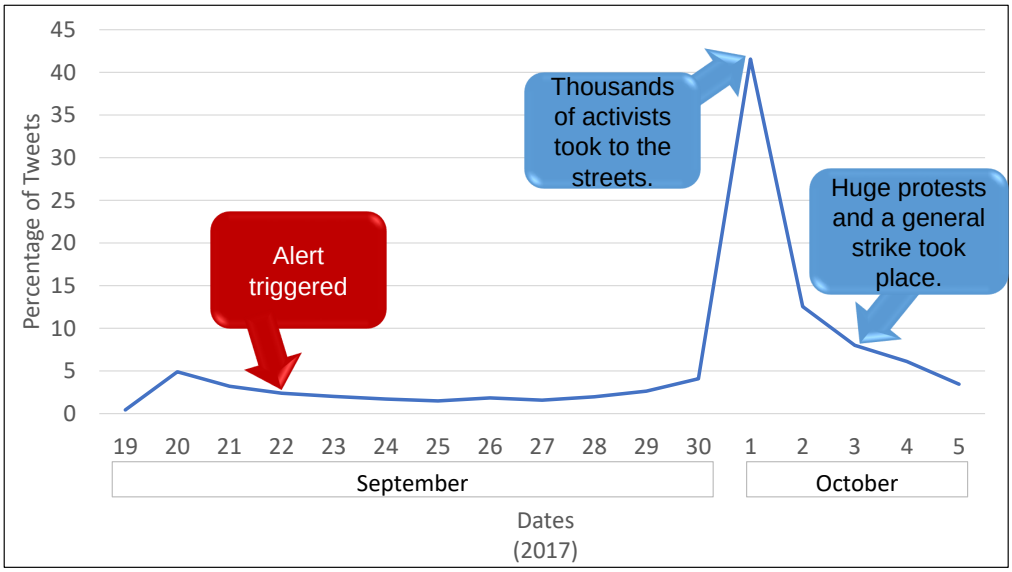


Figure 6.4: Tweet distribution during the massive protests in Catalonia.

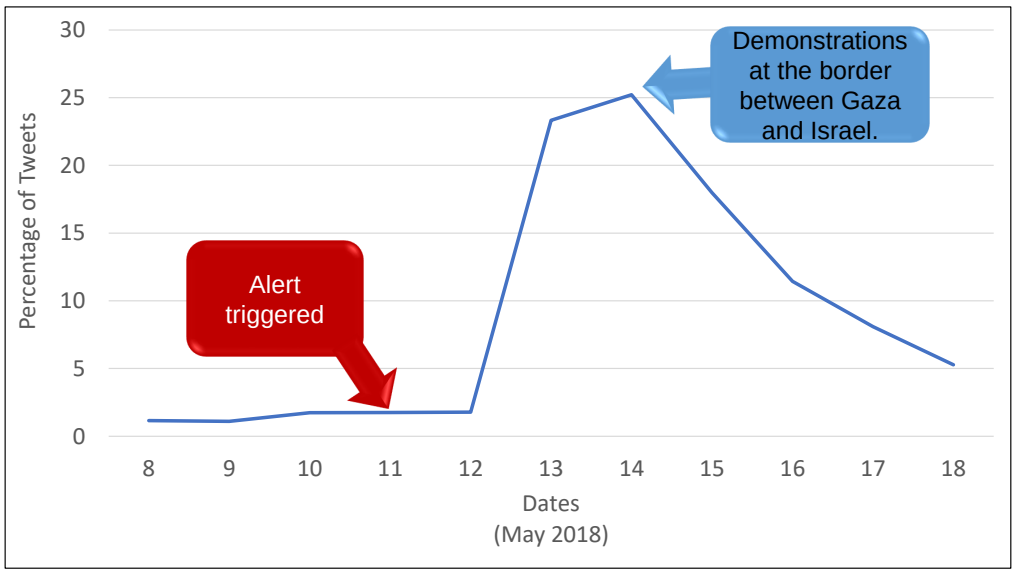


Figure 6.5: Tweet distribution during the demonstrations at the border between Gaza and Israel.

As mentioned in the previous subparagraph (Polarisation Analysis), sentiment analysis was performed to visualise which sentiment played the leading role, as Figure 6.6.I and Figure 6.6.II depict, negative perceptions had the prime position. Such a result can be explained in view of the fact that both events are related to unrests.

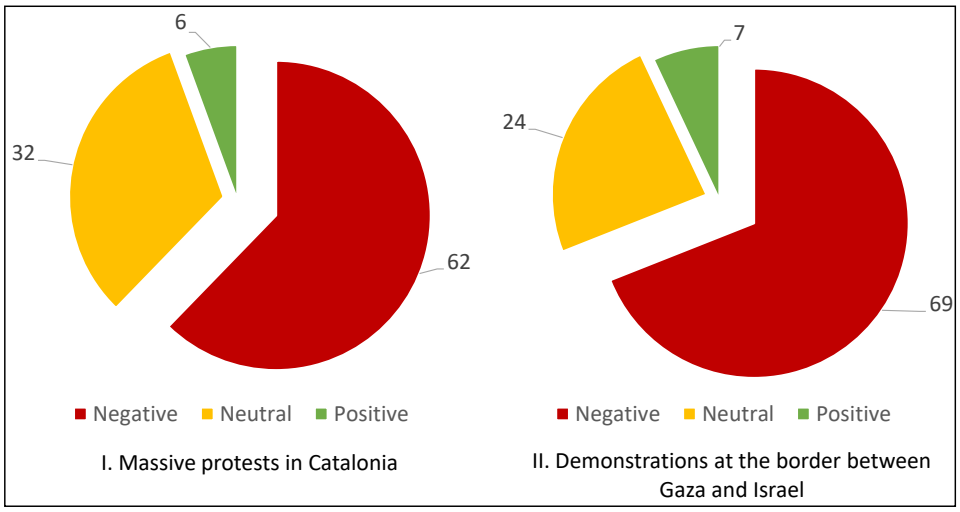


Figure 6.6: Percentage of sentiments (Protests in Catalonia and Demonstrations in Gaza).

However, one factor that needs to be observed is the time frame which will be considered as the preliminary one to carry out the training and threshold calculation process. Hence, the early alert mechanism proposed in Chapter 4 and explained in [89] was used to select such a time period, which ranged from the initial date up to the spotted tipping point, see Figures 6.4 and 6.5.

Social instability affects numerous factors of state life, and national security is unbalanced when human security components are affected [7,67]. To identify such a type of disturbances in our data corpora, a document classification model was used to categorise tweets into the eleven aspects of human security. Word embeddings together with the Gradient Boost Machine technique were implemented, in a similar fashion to Chapters 4,5 and 6 [89, 109, 133].

In addition to the document classification process, one important angle lies in disassociating those human security aspects that contribute to describing the event from those that do not add relevant information to delineate it. In order to dis-

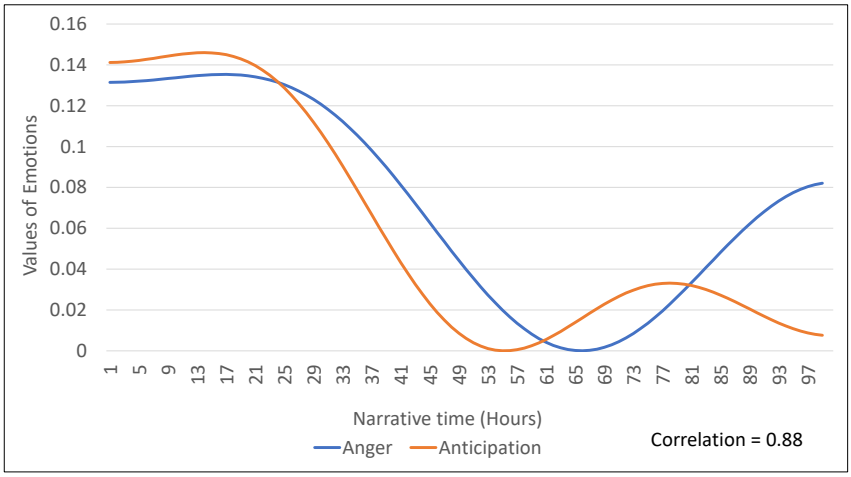
tinguish these aspects, the factor analysis method was used, which is focused on analysing relationships and patterns, as explained in [134]. The results from this process suggested that in both cases (protests in Catalonia and demonstrations in Gaza), only four of the eleven components were significant, namely government, public order, defence, and health.

Section 6.3 described the way dyads are calculated from the wheel of emotions proposed by [63]; ergo, the NRC emotion lexicon suggested by [135] (anger, fear, anticipation, trust, joy, disgust, sadness and surprise) were used to compute the individual emotions of both authoritarianism and hostility, by clustering tweets based on two aspects: date and hour.

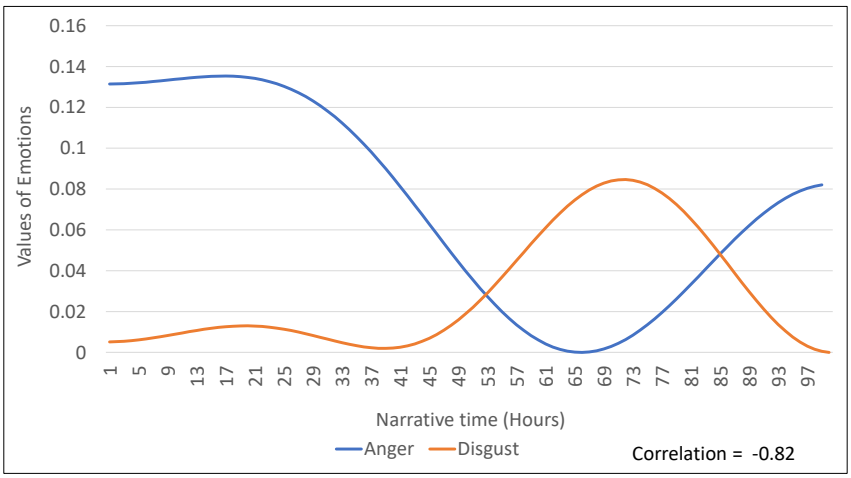
The resulted emotion values were then transformed by using the Discrete Cosine Transformation, which converts data from a spatial domain into a frequency-domain, as in [136]. The reason this process was performed is that analysing the similarity between the transformed emotion values discloses whether a dyad is present or not. As a result, the similitude between emotions was computing by a correlation process, where a high correlation value suggests that the dyad is significant, and individuals are conveying complex emotions as aggressiveness or contempt, see Figure 6.7.

Figure 6.7.I depicts a correlation of 0.88 which suggests that individuals were conveying posts nuanced by aggressiveness; by contrast, Figure 6.7.II illustrates a correlation of -0.82, which indicates that people were not sharing contempt-related messages during the incident.

While an incident evolves, there are time frames when emotions arouse due to abrupt situations, thus yielding complex emotions as submission, conventionalism or aggressiveness; however, detecting such unexpected behavioural patterns is not a trivial task. Therefore, identifying such a type of unforeseen patterns from the correlation outcomes described before can unveil traits of authoritarianism (submission, aggressiveness and conventionalism) and hostility (anger, contempt and disgust), which can be seen as anomalies. As a result, an anomaly detection process was performed by injecting the resulting correlation values of the emotional components of authoritarianism (aggression, submission and conventionalism) and hostility (anger, contempt and disgust) into a matrix, as illustrated in Figure 6.8.



I. Aggressiveness



II. Contempt

Figure 6.7: Discrete Cosine Transformation of emotions. Figures depict how emotions behave over time. Emotions are then correlated, and strong correlation values suggest that a particular dyad is present (i.e. aggressiveness, contempt, submission or conventionalism).

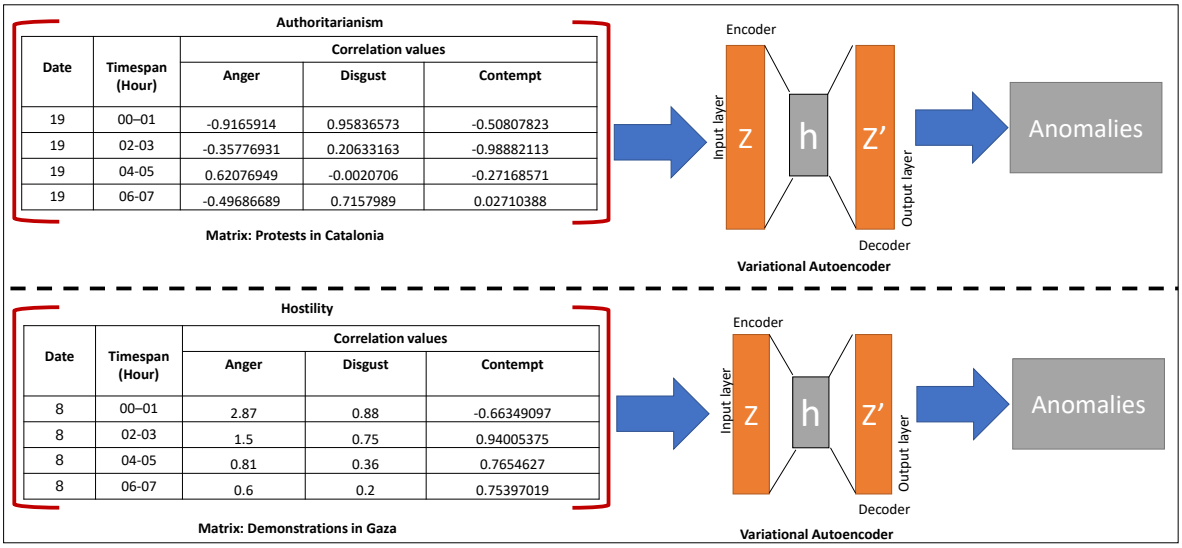


Figure 6.8: Emotion matrix example and anomaly detection process using a variational autoencoder.

Subsequently, these set of values were fed into a variational autoencoder model [137]. This unsupervised deep learning Generative Model was selected since it encodes input data to a low-dimensional latent space. Afterwards, a decoding process restores the data. Then, anomalies are detected by computing the mean squared error (MSE) between the original data and the output of the decoder, see Figure 6.9.

As illustrated by Figure 6.9.I and Figure 6.9.II, data as to aroused suspicious were extracted (anomalies) for both datasets the protests in Catalonia and the demonstrations in Gaza. This step was replicated for both authoritarianism and hostility. Finally, thresholds for both ideological traits are represented by the calculation of the mean of the two studied incidents, see Table 6.3.

As listed in Table 6.3, the proposed thresholds will work as a baseline to identify when an incident is dealing with both authoritarianism and hostility traits.

6.4.3 Information Extraction

Following the methodology workflow depicted in Figure 6.3, the information extraction process is fed by the thresholds computed during the previous step. However, when analysing a new data corpus, preprocessing text methods are required, which

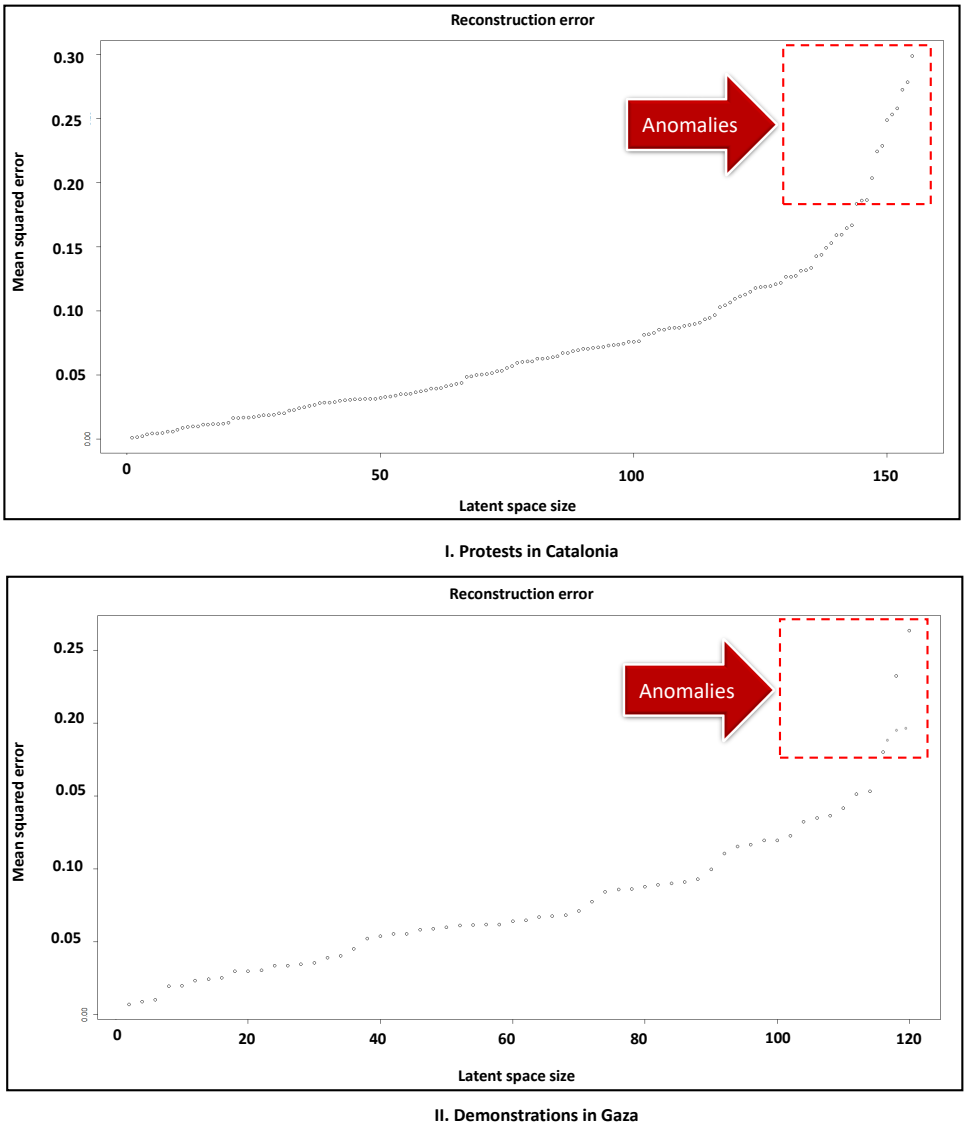


Figure 6.9: Mean squared error calculation of authoritarianism.

Table 6.3: Authoritarianism and Hostility thresholds.

Event	Authoritarianism			Hostility		
	Aggressiveness	Submission	Conventionalism	Anger	Contempt	Disgust
Catalonia	48	50	42	55	195	59
Gaza	61	64	55	59	165	135
Median	54.5	57	48.5	57	180	97
(Threshold)	T1	T2	T3	T4	T5	T6

is why the transformations proposed in the data ingestion process help to reduce future errors along with controlling the quality of the data that will flow throughout the entire procedure.

Secondly, as explained in [138], a post nuanced by violence or hate expressions has survival rates within the first twenty-four hours following the incident. For the purpose of this work, the aforementioned survival rate will be considered as a parameter to analyse likely disruptive events.

Thirdly, and in connection with this time parameter, the new data corpus is segmented per day/hour, and afterwards, emotions and dyads are calculated based on the methodology outlined above.

Fourthly, dyads and emotions are evaluated in accordance with the Algorithm 2.

```
Data: Tweets/Emotions
Result: Authoritarianism and Hostility
/* Thresholds:  T1= Aggressiveness; T2= Submission; T3= Conventionalism;
   T4=Anger; T5=Contempt; T6=Disgust                                    */
Begin
For ( hour in hours )
if Aggressiveness >= T1 then
    if Submission >= T2 then
        if Conventionalism >= T3 then
            if Anger >= T4 then
                if Contempt >= T5 then
                    if Disgust >= T6 then
                        Trigger an ideological trait day/hour
                    end
                end
            end
        end
    end
end
```

Algorithm 2: Ideological trait analysis.

6.4.4 Hashtag Analysis

Internet forums and in particular social media has changed the world dramatically, as the latter has been adopted at a fast rate worldwide, but during crises or disasters, the usage of such technological tools tend to explode [2]. In addition, the success that social media channels offer is supported by the opportunity to spread messages using short words or phrases which are succeeded by a hash pound (#), called hashtag [139]. Therefore, hashtags gain a core role since they enable to spread labelled messages, and where its dissemination intensity fluctuates while the event evolves.

As a result, understanding the semantic structure of a hashtag can provide additional information to construe the studied incident. In line with this idea, the semantic dissection process requires two main components. Firstly a verb that denotes a specific action, and secondly a noun that can refer to a person (P), object (O), location (L), or event (E), see Table 6.4.

The POLE model as proposed in [140] [141]), and which is based on the four elements previously described was selected because it depicts which are the critical entities/elements that individuals can include when a message is conveyed, and due to such a model is considered by authorities [142], see Figure 6.10.

Table 6.4: Example of entities in the POLE Model. Adapted from [140, 141].

Hashtag selection POLE Model	
Type	Example
People	President, Deputy, Vice president
Object	Weapon, Food, Ammunition
Location	Country, Town, Human settlement
Event	Protest, March, Concert

Verbs, on the other hand, manifest actions directed towards a person, object, location or event, and the classification proposed by [60] generates a broad categorisation of activities which includes verbs of killing, want verbs or verbs of communication, see Table 6.5.

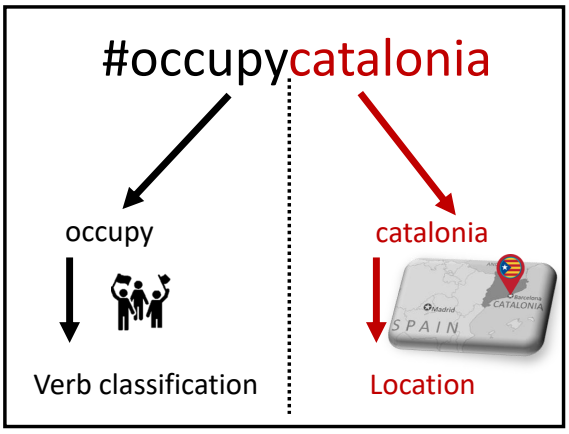


Figure 6.10: Hashtag analysis example.

Table 6.5: Example of verbs that enable the interpretation of actions, Adapted from [60].

Verb classes	Example
Build verbs	Build, Arrange and Churn
Verbs of change of state	Crash, Break and Shatter
Verbs of communication	Explain, Say and Convey
Verbs of contact by impact	Bang, Beat and Strike
Fill verbs	Block, Bombard and Flood
Want verbs	Need, Want and Hope
Verbs of future having	Feed, Give and Donate
Verbs of psychological state	Affect, Arouse and Agitate
Verbs of social interaction	Argue, Combat and Clash
Verbs of creation	Build, Assemble and Bake
Verbs of killing	Eliminate, Immolate and Liquidate

As shown in Figure 6.10, verb classification together with an entity (person, object, location or event), provide an enriched idea about an activity. For this specific case, to occupy a location named Catalonia.

In order to construe the intention that is behind a hashtag, the procedure described in the next two subsections is proposed.

1. **Entity Extraction**:

   As detailed in [140, 141], POLE elements represent a particular type of information which a specific activity is performed upon. Therefore, verbs that embody a variety of actions contribute to creating a holistic view while examining national security instabilities. A good illustration of the former topic is the analysis of both violent and non-violent actions, so as detailed in [82] there are some actions linked to these type of events as shown in Table 5.3.

   A critical step in our approach lies in bonding the variety of actions previously mentioned, together with the verbs listed in [60], to create an enriched lexicon of verbs. Table 6.6 displays a list of violent and non-violent verbs. This selection is an adaptation of the verbs embedded in the phrases depicted in Table 5.3 , and that match the classification proposed by [60].

   Apart from the specialised lexicon of verbs, entities as people, location, objects or events, are the second factors to be extracted. However, as there are a vast number of entities, one way to narrow them down radicates in considering only those who are surrounding the area where the event takes place.

   Using a knowledge base as Wikidata or Wikipedia provides an alternative path for querying the forenamed entities, but a significant aspect lies in selecting a list of the strategic ones. Hence, to create a robust catalogue, the entity classification list proposed in our previous work [109] was considered. The selected catalogue includes human settlements, critical facilities, food, objects, companies and people, and in order to enhance the object extraction, a dictionary based on weapons was also added, as listed in [143].

2. **Semantic Matching**:

Once the lexicon of verbs and the entity dictionary (POLE) are created, a string matching process is performed according to the sequence of steps outlined below:

* Verb Analysis. Firstly, hashtags are matched against the lexicon of verbs previously created, then those hashtags that contain the verbs listed are selected. Subsequently, verbs are separated from the rest of the string.
* Entity Analysis. The remaining string is matched against the entity wordlist created above using a phonetic algorithm as SoundEX since it analyses the pronunciation as detailed in [106], contributing in such a way to detect spelling errors.
* Phrase Analysis. Extracting the narrative that is associated with the selected hashtags by boiling down the information of all tweets linked to them, unveil a different level of strategic data. Therefore, the data analytics methodology proposed in our work [133] focused on extracting noun phrases using techniques as word embeddings will be used.

Table 6.6: Example of verbs linked to violent and non-violent actions. Adapted from [60, 82].

Verb Description	Activity	
	Violent	Non-violent
Immolate	✓	X
Liquidate	✓	X
Clash	✓	X
Block	X	✓
Strike	X	✓
Arrest	X	✓

6.5 Experiments and Validation

A real-life event can create a suitable atmosphere to test the robustness of the proposed methodology, as well as its linked processes and algorithms. Consequently, protests that erupted in Puerto Rico in July 2019 as a result of an alleged government texting scandal was chosen [144, 145]. The selection of this disruptive event was centred on its particular nature that involved massive protests due to internal problems, and because national security components were unbalanced accordingly.

6.5.1 Data Ingestion

The analysed data corpus comprised from July 11th to 25th 2019, and it was collected selecting hashtags considered as trending ones, using the historical Twitter API. Figure 6.11 displays a schematic view of the dataset to be analysed.

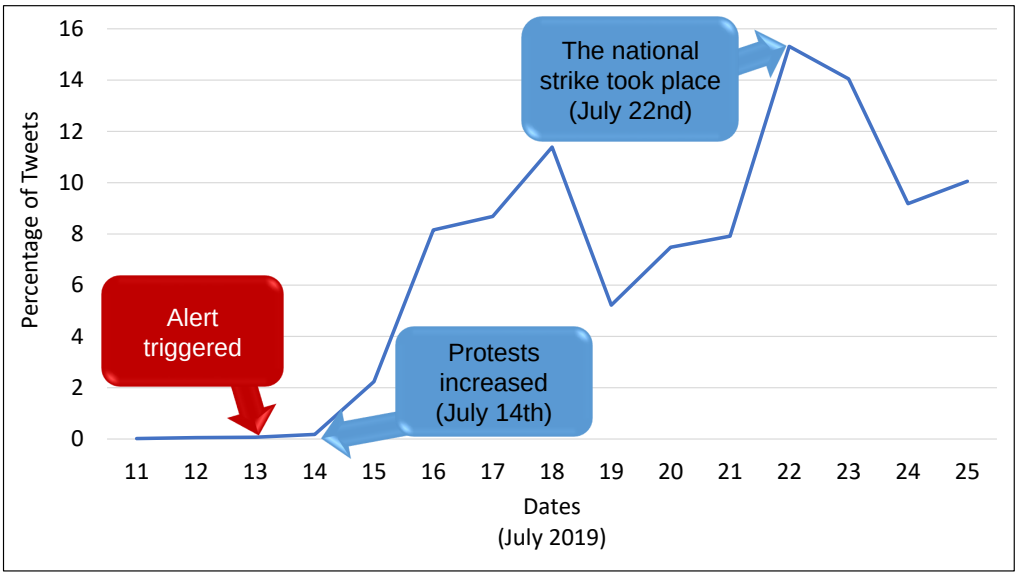


Figure 6.11: Tweets from the incident in Puerto Rico (July 2019).

As a first step, the alert mechanism described in Chapter 4 [89] was used, aimed at spotting the potential beginning of a tipping point. It can be seen in Figure 6.11 that an alert was triggered on July 13th. 2019, a day before protests grew.

Secondly, sentiment analysis was performed to verify which sentiment was leading the incident (see Section IV). As depicted in Figure 6.12, negative sentiments have a predominant role as they represent 71%.

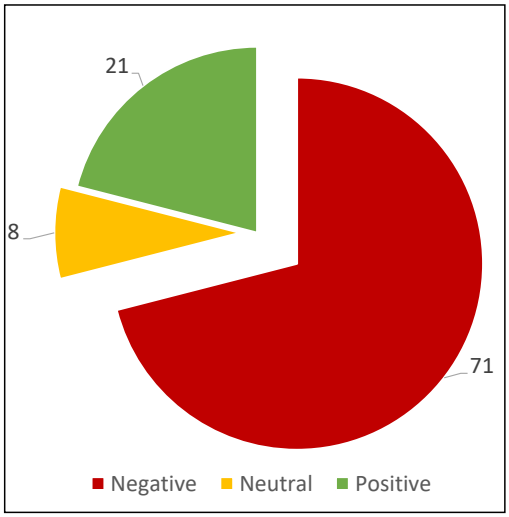


Figure 6.12: Percentage of sentiments (Puerto Rico).

6.5.2 Information Extraction

Thirdly, following the information extraction process detailed in Section 6.4, emotions and dyads were calculated. As illustrated in Table 6.7, five ideological spots were identified during five different dates. The first one was pinpointed just the same date when the alert mechanism was triggered and a day before protests increased. Such a result draws a red flag, as [115] indicates that authoritarianism is linked to the prediction of disruptive attitudes. In a similar fashion to [114, 124] where the triad of the hostility traits announces the prelude of a crisis.

Table 6.7: Results of Emotions and Dyads (Puerto Rico).

Date	Timespan	Authoritarianism			Hostility		
(July)	(Hour)	Aggressiveness	Submission	Conventionalism	Anger	Contempt	Disgust
13	0400-0500	77	70	95	70	180	99.6
15	2200-2300	98	59	88	300	190	310
17	0600-0700	73	72	76	76	220	338
19	0400-0500	69	62	98	133	180	113
20	0200-0300	97	95	87	300	195	285

A day after protests escalated, ideological traits continue to appearing; however, on July 15th hostility figures had a significant increase of 182% on average and au-

thoritarianism had a modest growth of 1.39% on average. This result suggests those collective emotions that denote appraisals of inferiority, injustices, or intolerability were present, as described in [114, 124].

Moreover, two days before the national strikes took place (July 22nd); ideological traits appeared again. This result becomes relevant since hostility traits had a substantial increase of 95.36% on average and authoritarianism had a considerable climb of 28% on average, which suggests that a second red flag was present.

6.5.3 Hashtag Analysis

Finally, the hashtag analysis procedure was carried out as outlined in Section 6.4, using five datasets that correspond to the dates where the ideological traits were found (see Table 6.7).

As displayed in Table 6.8, three leading hashtags were posted while the incident erupted such as "resignricky", "rickyleaks" and "puertorico". Regarding the first text label (resignricky), it is comprised of two elements, a verb that refers to resignation, and an entity that is connected to a person, in this case, a governor according to the Wikidata knowledge base. By contrast, the narrative that is linked to the former hashtags presented dissimilar views. For instance, the date when the tipping point was spotted (July 13th) tweets that were spilt on social media were demanding the resignation of an entity (governor), and at the same time were expressing that protesters were harassed. The following date protests increased (July 15th), messages associated with demanding the resignation of the entity mentioned above, and a feeling of claiming dissatisfaction were also disseminated.

Lastly, from July 19th-20th, a couple of days before the national strikes explode (July 20th), posts that evoked the use of telegram as a mean of communication were conveyed, along with actions such as threw cans, ignited fireworks, looting, impeachment and the request for resignation.

If this methodology had been utilised when this incident occurred, a big picture of the ideological traits would have helped to construe the evolution of the event and to decide the best course of action to address the situation.

Table 6.8: Hashtag Analysis (Puerto Rico).

Date	Hashtag (#)	Verb	Verb Description	Entity (Wikidata label)	Information Summary (Data Analytics)
13	Resignricky	resign	Non-Violent	Ricky (People:Governor)	Harrasing ==>Protester Demand ==>Resignation
	Rickyleaks	leaks	Non-Violent	Ricky (People:Governor)	
	Puertorico	-	Non-Violent	Puerto Rico (Location: Territory)	
15	Resignricky	resign	Non-Violent	Ricky (People:Governor)	Demand ==>Resignation
	Rickyleaks	leaks	Non-Violent	Ricky (People:Governor)	Claim ==>Dissatisfaction Harrasing ==>Protester
	Puertorico	-	Non-Violent	Puerto Rico (Location: Territory)	
17	Resignricky	resign	Non-Violent	Ricky (People:Governor)	Want ==>Impeachment Demand ==>Resignation
	Rickyleaks	leaks	Non-Violent	Ricky (People:Governor)	Install ==>Blockade Set ==>Roadblock
	Puertorico	-	Non-Violent	Puerto Rico (Location: Territory)	Gassed ==>Protester Want ==>Resignation
19	Rickydisappear	disappear	Non-Violent	Ricky (People:Governor)	Use ==>Telegram
	Resignricky	resign	Non-Violent	Ricky (People:Governor)	Demand ==>Resignation Make ==>Loot
	Rickyleaks	leaks	Non-Violent	Ricky (People:Governor)	Ignite ==>Firework Throw ==>Can
20	Rickydisappear	disappear	Non-Violent	Ricky (People:Governor)	Seek ==>Resignation Exploit ==>Uprising
	Resignricky	resign	Non-Violent	Ricky (People:Governor)	Demand ==>Resign Want ==>Resignation
	Rickyleaks	leaks	Non-Violent	Ricky (People:Governor)	Gassing ==>Protester Throw ==>Can

6.6 Conclusion

This chapter has introduced a data analytics methodology to identify and unveil ideological features (authoritarianism and hostility) to construe national security instabilities by using a variety of computational techniques (NLP, machine learning and deep learning models). The proposed workflow includes three main steps, training and threshold calculation, information extraction and hashtag analysis, as depicted in Figure 6.3.

In order to train the ideological mechanism, two events were processed, and as a result, a set of thresholds were computed for authoritarianism and hostility. By using such figures, new spots of ideology were detected in a different incident, namely, the protests in Puerto Rico in 2019. Moreover, to enrich the analysis, the hashtag examination process helped to unveil aspects such as actions and entities (people).

Chapter 7

Big Data for National Security in the Era of COVID-19

7.1 Introduction

Global challenges and emergencies such as climate change, epidemics and natural and man-made calamities present unprecedented governance issues. The COVID-19 pandemic has demonstrated how a global challenge can disrupt more than 180 countries [146]. Governments across the globe have taken strict decisions aimed at containing the disease and avoiding massive infections, such as curfews, lock-downs, "stay at home" orders, or compartmentalization of domestic territories according to their infection rates [147].

Such measures represent a meaningful way to control the disease, however, they also have a negative effect on people's lives imposing dramatic changes in the ways of life people had been used to. As a result, containment measures have often be met with varying degrees of social discontent and unrest, from protests and non-compliance actions to more violent manifestations such as demonstrations and riots [148]. A state's stability could be seriously undermined by such social instability incidents, which may have a negative effect on national security components such as health, economy, and public order [7].

Policy and decision-makers need to have at their disposal technological tools, acting as force multipliers and enabling insights about disasters and unfolding situ-

ations, so that an assessment of the scale of the threat to national and international security can be made [149,150]. Big Data technologies can provide a powerful means in this endeavour [151,152]. As a result the last decade we have witnessed the development of several computational platforms that utilise Big Data analytics to derive insights about disruptive situations that can trigger social unrest [28–30, 153–155].

In line with this aspect in previous chapters, the conceptual framework and the associated workflow for the analysis of social media data (Twitter) to derive insights about disruptive events and potential unrest have been presented [67, 89, 109, 133, 156]. In this chapter, this framework is utilised to analyse the COVID-19 pandemic. The analysis focuses on two geographical areas where acts of social unrest were witnessed as a result of COVID-19 containment measures, namely Michigan and Texas.

The aims and contributions of this chapter are twofold. Firstly, to demonstrate the robustness and applicability of our framework for forecasting and analysing important real-world events such as COVID-19 related unrest: would the framework have been able to provide the competent authorities enough notice and insights to deal with the then unfolding crisis? Secondly, to provide postmortem insights about COVID-19 social crises, which can be delivered to interested stakeholders to create a big picture of the situation.

7.2 COVID-19 and National Security

National security threats refer to those activities that endanger the individuals' physical well-being, or compromise the stability of the state. When we place people at the centre of the analysis of how national security is affected, in which case it is also referred to as human security, we typically distinguish between seven different components: economic security, food security, health security, environmental security, personal security, communal security and political security [7]. Instabilities are generated due to the disruption of one or more these components leading to protests, riots and other forms of violence [67, 157]. According to the Global Peace Index [8], civil unrest has doubled over the past decade, and riots, strikes and anti-government

protests increased by 244%.

Countries around the world define their domestic security threats based on their internal policies. Pandemics are typically considered national security threats due to their negative social, economic and political impacts [158]. As a global pandemic, COVID-19 represents a serious National Security threat [159]. The negative social and economic effects of lockdowns and curfews have fuelled preexisting social discontent and unrest (e.g. in the Black Lives Matter movement, or the demonstrations in Hong Kong) as well as new anti-lockdown demonstrations. These demonstrations, in turn, act as super-spreader events, further exacerbating the negative impacts of the pandemic [160].

7.3 An Overview of the Framework

The methodology described in previous chapters [67, 89, 109, 133, 156], attempts to enrich the security decision-making process scenario. It analyses national security considering its broad spectrum components, including but not limited to health and public order; enabling in such a way to detect timely tipping points and examine a variety of situations as riots, protests or events linked to health issues such as COVID-19.

As described before, the framework consists of two main stages (see Figure 3.2) An initial phase (Warning Period) continuously analyses data and issues an alert when it identifies that specific societal behavioural characteristics exceed a given threshold (tipping point). The system then gets into its next phase (Crisis Interpretation) by collecting information from numerous sources, such as social networking services or websites, to attempt to zoom in and provide more in-depth insights that unveil data to construe the unfolding crisis and support therefore authorities and other stakeholders into making better decisions.

Under the new normal, where COVID-19 tends to modify critical behavioural aspects of people's lives, understanding features that directly impact the security of a state becomes crucial. Here, the aim is to use features extracted from the conceptual framework to interpret the health crisis. The characteristics used in this

chapter are summarised in Table 7.1.

Table 7.1: Insights derived from the Analytics Framework described in [89, 109, 133, 156].

Insights		Stages			
		Early Warning Alert	Radical Behaviour	Ideology	Web Insights
Q1.	When do people head towards a situation that evokes that both social stability and national security components can be compromised?	✓	-	-	-
Q2.	Which entities are described by people during the crisis?	-	✓	-	-
Q3.	What are the radical behavioural traits being conveyed?	-	✓	-	-
Q4.	What items are being asked for by individuals in social media?	-	✓	-	-
Q5.	Are hostility and authoritarianism traits present during the incident?	-	-	✓	-
Q6.	Do embedded web resources in social media texts disclose that the national security components have a horizontal escalation over time?	-	-	-	✓

7.4 Analysing Two COVID-19 disruptive events

As stated in previous chapters, the conceptual framework's main objective is to monitor the state of the society at any particular moment and, in case of an alert, to derive deeper insights about the situation and the threat it may constitute to national security. With this goal in mind, two incidents of social unrest, which occurred in April 2020 in Michigan and Texas, are studied, both related to COVID-19 outbreak.

The two events were chosen in consideration of the people's reactions. In both cases, citizens protested after local governments adopted lockdown rules, notwithstanding the strict restrictions imposed to tackle the pandemic.

In the case of Texas, rallies were organised to show disagreement against local restriction measures, and people demanded to reopen the economy [161, 162].

By contrast, in Michigan, a convoy of thousands of motorists drove from all over the state to protest the governor's stay-at-home order extension. The protest, known now as Operation Gridlock, involved clogging with their vehicles the streets surrounding the Michigan State Capitol, including the Capitol Loop, and drew national attention [163].

7.4.1 Data Collection and Cleansing

A data corpus of six million tweets written in English was collected from 10th to 20th April 2020, by considering hashtags such as #covid, #coronavirus, #coronavirusoutbreak and #coronaviruspandemic. Then, two data subsets were extracted from the anterior dataset, each subset containing tweets with a unique combination of specific parameters, such as hashtags that were linked to the studied entities (locations), as depicted in Table 7.2.

Once these two subsets have been created, tweets appertained to the former clusters were cleansed following the steps described below: (1) URLs were extracted; (2) RT and mention terms were removed; (3) contractions were replaced, for instance, wasn't: was not; (4) punctuation marks were removed; (5) emoticons were replaced by words; (6) Internet slang was replaced by complete expressions using a preconfigured dictionary, for example, AFAIK: "as far as I know", ASAP: "as soon as possible", or BBL: "be back later".

7.4.2 Early Warning Alert (Q1)

Once an incident is unfolding, the stability of the state can be compromised due to national security components instability, at which point identifying if an event heads toward a significant disruption scenario becomes a primary task. In light of this, the analysis of three indicators, namely, Global Polarisation, Social Media Connectedness and Human Security Impact, enable the identification of the real nature of the event by triggering an early warning alert, as described in Chapter 4

Table 7.2: Popular hashtags posted on April 2020 linked to two locations, namely, Michigan and Texas. The depicted hashtags in the table involve two tokens, the first one associated with a location and the other with a noun/verb. The two types of tokens are shown in different colours - red and black.

Dataset 1 (Michigan ,USA)		Dataset 2 (Texas, USA)	
#michigan	#michiganlockdown	#texas	#stayhometexas
#liberatemichigan	#freemichigan	#opentexas	#texasstrong
#michiganprotest	#michiganshutdown	#reopentexas	#texans

and in [89].

1. **Michigan**:

   Figure 7.1 shows that the system would generate an alert on 14th April 2020, a day before protests began because the governor's "stay at home" order was declared, and five days before protests escalated (19th April 2020). The triggered alarm suggests that the internal cohesion amongst national security components has been disrupted.

2. **Texas**:

   As depicted in Figure 7.2 on 11th April 2020, an alert was triggered by the early warning process, eight days before protests against Coronavirus policies intensified (19th April 2020).

7.4.3 Radical Behaviour (Q2, Q3 and Q4)

The analysis of radical behavioural traits can lead to critical and actionable insights. Tables 7.3 and 7.4 demonstrate how addressing Q2, Q3 and Q4 enable the identification of entities, behavioural traits and required objects, justifying the use of the radical behaviour analysis methodology described in Chapter 6 [133] to enrich this part of the analysis.

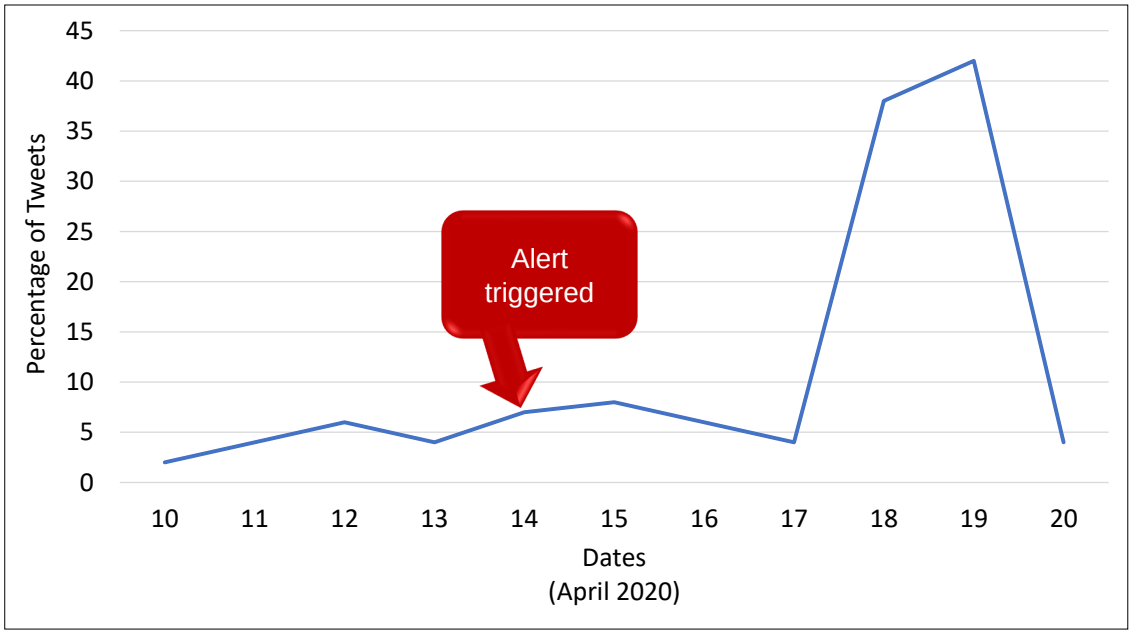


Figure 7.1: Tweet distribution and early warning alert detection during the protests in Michigan in April 2020 due to the COVID-19 restrictions.

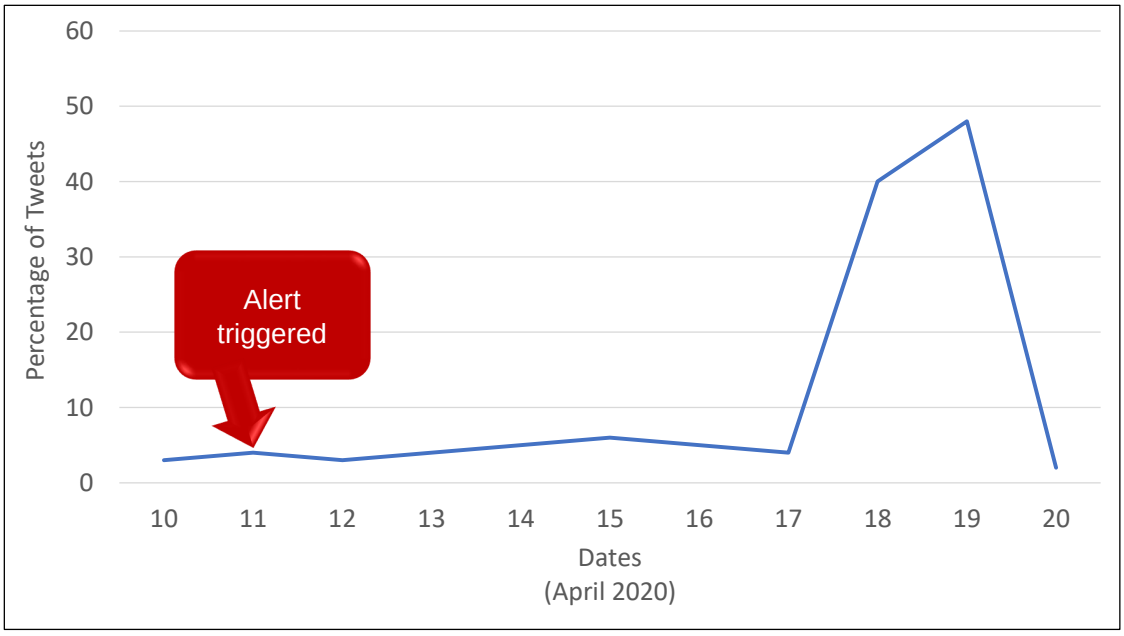


Figure 7.2: Tweet distribution and early warning alert detection during the protests in Texas in April 2020 due to the COVID-19 restrictions.

1. **Michigan**:

   Q2. and Q3. In order to facilitate the narrative, Q2 and Q3 will be pre-

sented together. It can be seen in Table 7.3 that on April 15th 2020 protesters were conveying messages about violating the lockdown as well as expressing disagreement against the measure. In contrast, two days later messages that expressed an intention to take to the streets were disseminated, coupled with messages that urged people to wear masks while protesting; moreover, messages suggesting the location of the protest, namely Michigan, were conveyed too.

On 18th and 19th April 2020, demands related to the lift of the lockdown and messages urging to continue protesting against the imposed measures were spread. In addition, some other ideas were present, such as demands to reopen, lift the quarantine, and liberate from the lockdown. Incitement to actions affecting various public thoroughfares, such as blocking roads or taking to the streets, were also present.

Q4. Lastly, messages were individuals conveyed their personal needs for PPE (personal protective equipment), or urge for action towards a cure for COVID-19 were shared likewise, see Table 7.3.

Table 7.3: Disruptive Expressions extracted using Word Embeddings and Direct Object (Michigan).

Location	Dates (2020)							
	April 10	**April 11**	**April 12**	**April 15**	**April 16**	**April 17**	**April 18**	**April 19**
Michigan				Violating ==>Lockdown		Stop ==>Insanity	Cancel ==>Lockdown	Avoid ==>Quarantine
				Disagree ==>Curfew		Take ==>Streets	Protest ==>Lockdown	Violating ==>Distancing
				Protest ==>Rally		Break ==>Demand	Take ==>Lockdown	Michigan ==>Edict
				Protest ==>Virus		Protest ==>Michigan	Protest ==>Distancing	Need ==>Lawmaker
						Wear ==>Masks	Demand ==>Reopening	Break ==>Curfew
						Shut ==>Now	Liberate ==>Lockdown	Want ==>Cure
							Block ==>Roads	Want ==>PPE
							Rally==>Arizona	Take ==>Streets

2. **Texas**:

   Q2. Radical behavioural traits revealed that individuals expressed ideas linked to reopening a specific location, namely, Texas, see Table 7.4. According to the Levin's classification [60], the verb "need" expresses that a person desires something. Following Levin's analysis, on April 17th 2020, messages were posted conveying the desire that a different location, Michigan, would join the incident. As argued in [82], this mention of different locations, suggests that the state is dealing with a widespread event.

   Q3. Social media users (Twitter) expressed concepts connected to the demand of allowing business in the city, lifting the quarantine, and contempt towards Coronavirus, as described in Table 7.4. On the other hand, in the following days (17th, 18th and 19th April 2020), messages that instigate violations of the lockdown, urge protest and boycott, close schools, wear PPE, and spread the frustration, were shared.

   Q4. Concerns about health were also transmitted, related for example to the need for more nurses, and the rise of deaths.

Table 7.4: Disruptive Expressions extracted using Word Embeddings and Direct Object (Texas).

Location	Dates (2020)							
	April 10	**April 11**	**April 12**	**April 15**	**April 16**	**April 17**	**April 18**	**April 19**
Texas		Allow ==>Business	Halt ==>Covid			Reopen ==>Government	Spreading ==>Frustation	Hoarding ==>PPE
		Avoid ==>Corona	Develop ==>Diarrhea			Need ==>Michigan	See ==>Outrage	Open ==>Quarantine
		Lifting ==>Quarantine	Open ==>Employment			Close ==>Schools	Wear ==>PPE	Observe ==>Distancing
		Reopen ==>Texas	Help ==>Employees				Wear ==>Facemask	Protesting ==>Coronavirus
		Care ==>Lives	Puts ==>Halt				Authorizing ==>Reopen	Violate ==>Lockdown
		Rise ==>Deaths						Protest ==>Lockdown
		Want ==>Nurses						Support ==>Boycott
								Make ==>Masks
								Rally ==>Whattsapp
								Rally ==>Austin Texas

7.4.4 Ideology (Q5)

The ideological traits of authoritarianism and hostility reveal important social characteristics. Authoritarianism denotes that individuals do not empathise with decisions or activities performed by those who hold the "proper authority" [164, 165]. Hostility enables the identification of collective emotions which are seen whilst disruptive events take place [124, 166].

In order to begin the dissection of ideology in the COVID-19 datasets, a sentiment analysis process was performed, then tweets with negative polarisation were selected accordingly. In both cases, negative sentiments played the predominant role; Michigan had the highest percentage with 51%, while Texas had 35%. Then authoritarianism and hostility traits were computed using the methodology and thresholds described in Chapter 7 [156] (see Figure 7.3).

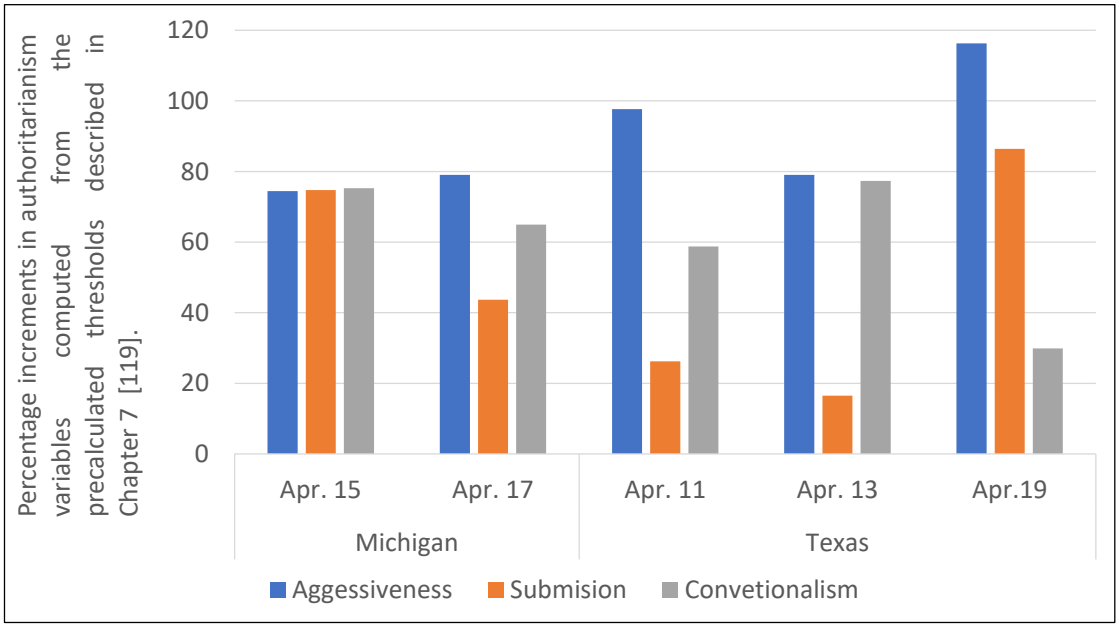
1. **Michigan**:

   A day after the early warning alert was triggered (April 14th 2020), signs of authoritarianism and hostility were detected (April 15th 2020), the same date that the local government imposed the lockdown, see Figure 7.3.I.

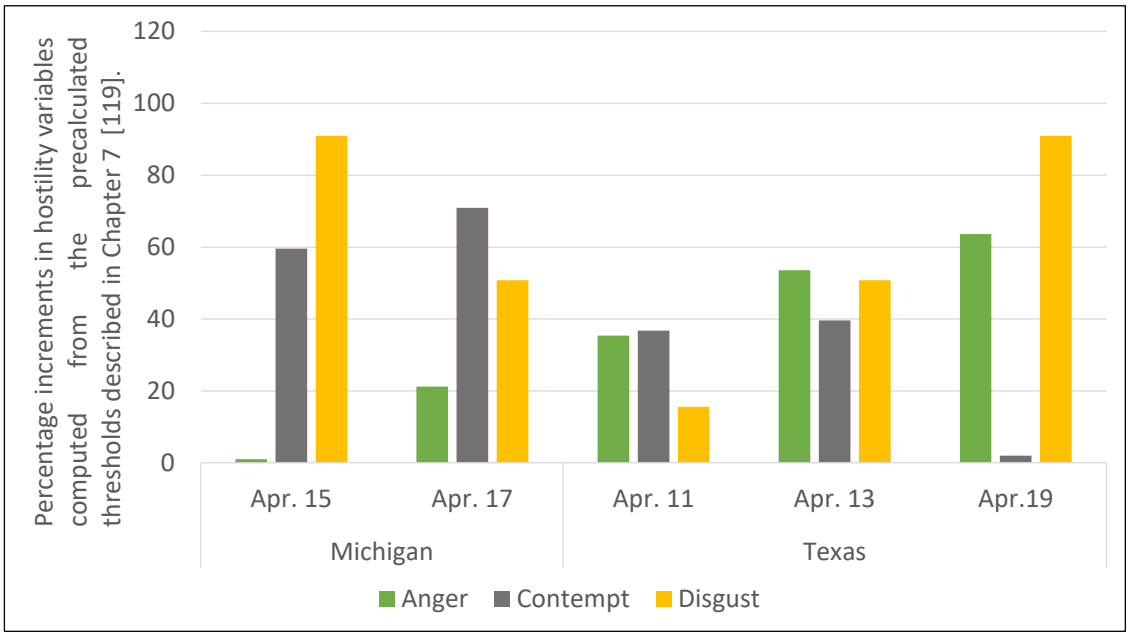
2. **Texas**:

   On April 11th 2020, ideological traits were detected, the same date that the early warning alert was triggered, see Figure 7.3. This specific point turns into a core axis, since people were concerned about aspects such as the COVID-19 death toll, and lifting the quarantine, see the radical behaviour analysis in subsection 7.4.3 and Table 7.4.

   Regarding authoritarianism, it should be noted that in both of the studied cases, aggressiveness was above 60% of the precalculated threshold, while the other two variables showed irregular increments. The consistent increase in aggressiveness suggests that people were conveying messages indicating prejudice/intolerance against a specific topic [165], here a lockdown, a curfew, or a quarantine, see Tables 7.3 and 7.4.



I. Authoritarianism



II. Hostility

Figure 7.3: Ideological traits (Michigan and Texas).

7.4.5 Web Insights (Q6)

During an incident or a health crisis such as COVID-19, individuals and organisations use digital channels to disseminate information and data such as breaking news, messages or pictures, the analysis of which can help understand whether a crisis is escalating over time. Hence, as described in Chapter 5 [109], the web insights methodology proposed enables the study of the horizontal escalation of national security components. Following the methodology there, URLs were classified according to a comprehensive list of entities created over the Wikidata knowledge base. Then, a web scrapping process was conducted to retrieve the content of such web resources.

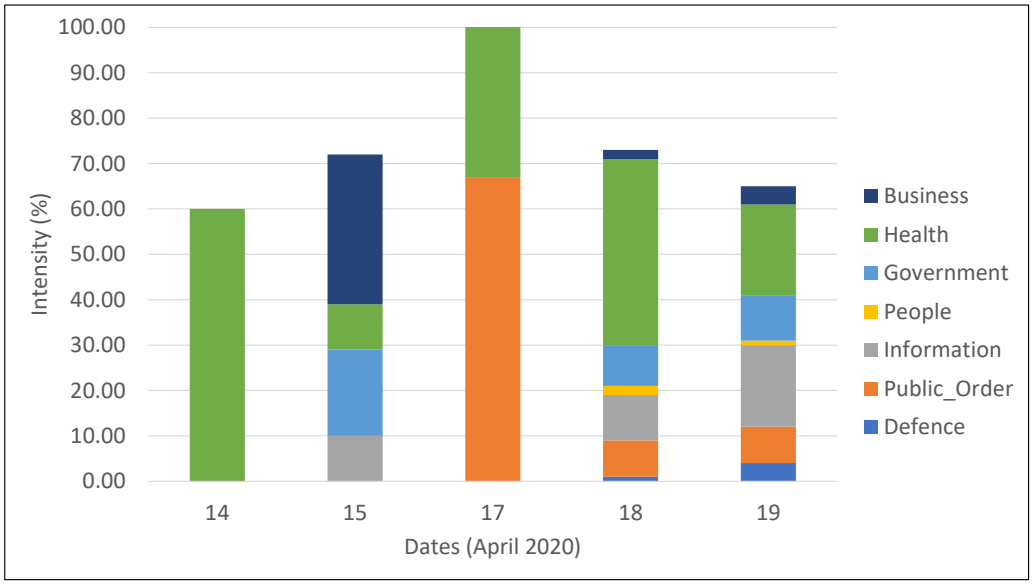
1. **Michigan**:

   It can be seen in Figures 7.4.I and 7.4.II, that only two media resources were embedded in people's messages while posting a tweet, namely Independent Websites (IW) and Social Networking Services (SNS).

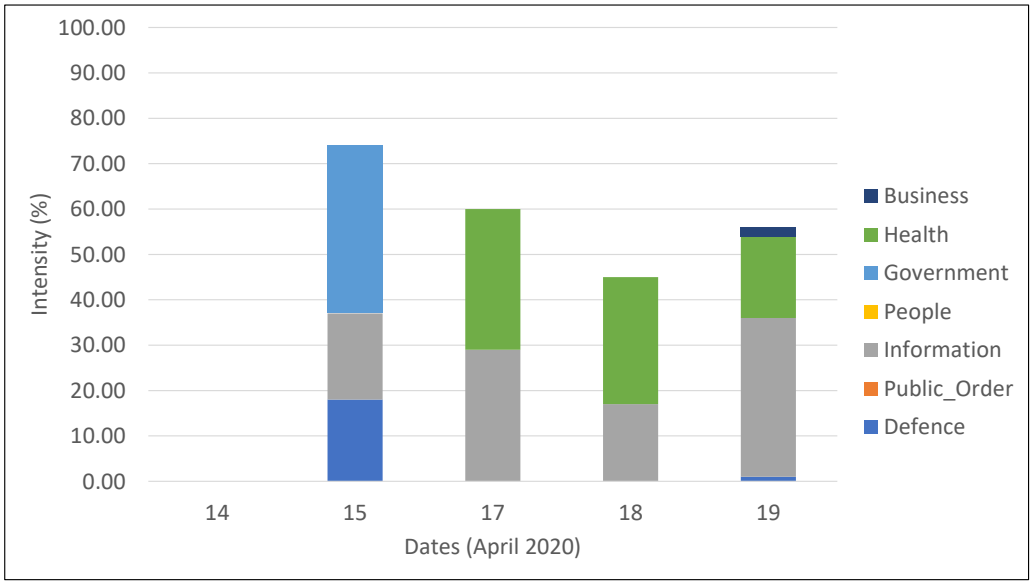
   On April 14th 2020, when the early warning alert was triggered, SNS (Instagram and Twitter) were used to convey that one national security component was being affected, in this case, health. One day later, messages posted on those social media sites showed that four national security components were unbalanced (information, defence, business and health). Such increment in the number of affected components (from one to four), demonstrates a horizontal escalation, which, according to [81] may represent a disruptive situation, see Figure 7.4.I.

   It should be noted that both business and government components had the highest intensities, which may complement the behavioural traits previously extracted that referred to violating the lockdown and the disagreement towards that measure (see Table 7.3).

   On the other hand, IW showed on April 15th 2020, that three national security components were affected, namely defence, information and government, and where this last component had the highest intensity figure. The result suggests



I. Social Networking Services



II. Independent Websites

Figure 7.4: Horizontal Escalation of the National Security Components during the protests in Michigan (April 2020).

that those web resources were providing a more detailed description of the government's activity (see Figure 7.4.II).

On the following days (17th, 18th and 19th April 2020), both IW and SNS published content affecting the health and information components. The result is relevant since, on April 19th, COVID-19 cases began to spike [163]. By contrast, only SNS revealed information about two other components (people and public order), as displayed in Figure 7.4.I.

2. **Texas**:

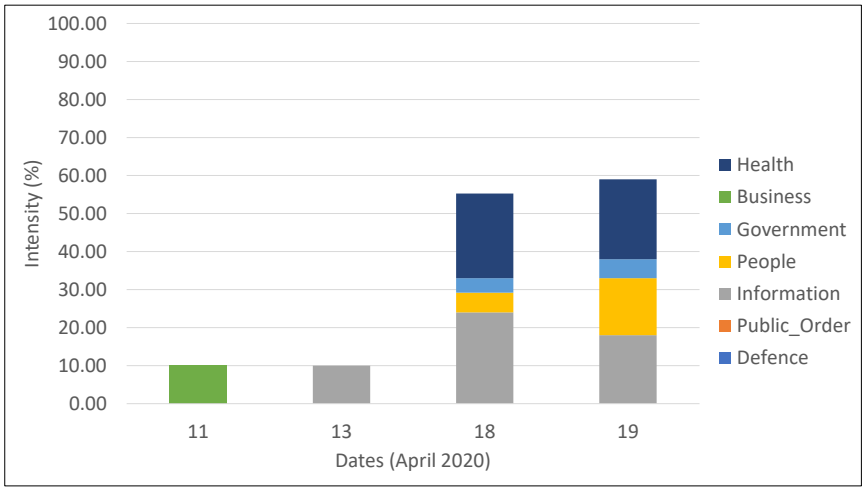
   Figure 7.5.I, 7.5.II and 7.5.III show that three digital web resources were used by people to disseminate information amidst the protests, namely, IW, SNS and Non-Profit Organisations.

   As mentioned earlier, the early warning alert and the emergence of ideological traits happened on the same date (11th April 2020). Unlike the previous case, the Independent Websites were used more intensively and they unveil that two national security components were disrupted, business and health; while SNS showed that only the business component was affected, with 80% less intensity than in IW.

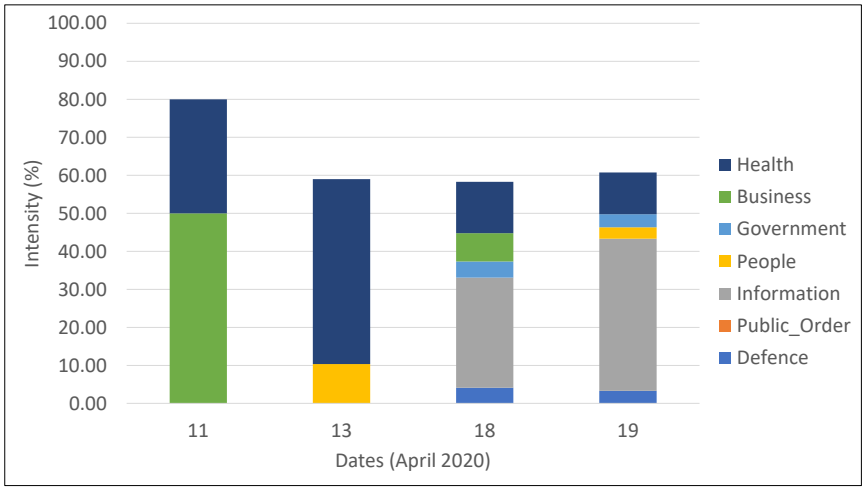
   Visible changes were displayed between 13th and 18th April 2020, as the IW and SNS showed an increased number of affected components, which exposed a horizontal escalation across the national security factors, which went from two affected factors to five for the IW, and from one to four for SNS.

   In addition, Non-profit organisations played a crucial role on the 18th and 19th April 2020, because topics in business and health were affected by them. Moreover, intensity health levels had a considerable increase of 85%, while, by contrast, health levels in SNS and IW showed little change, around 7% on average. Such a difference indicates that Non-profit organisations were stressing issues linked to health.

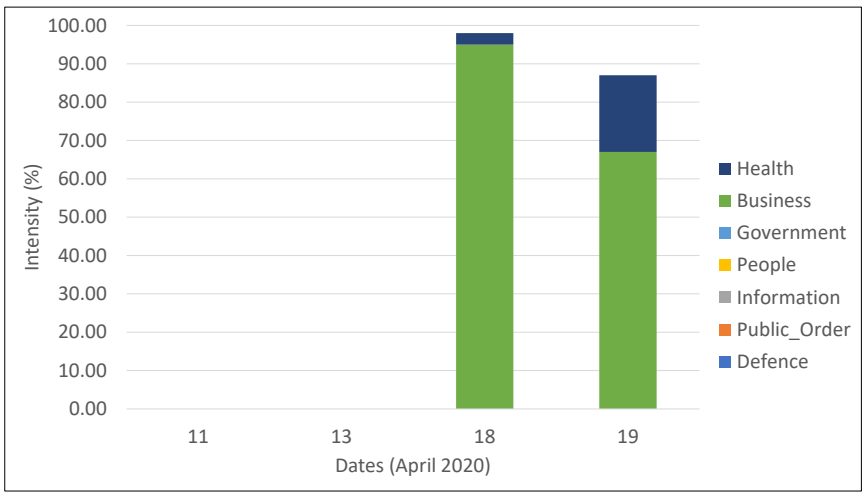
   Finally, it should be noted that on April 19th, when the highest burst of online activity took place (see Figure 7.2), SNS were used to convey more messages linked to people, as indicated by an increase of 70%; whereas IW were focused



I. Social Networking Services



II. Independent Websites



III. Non-profit Organisations

Figure 7.5: Horizontal Escalation of the National Security Components during the protests in Texas (April 2020).

on disseminating data related to the information component, which had an increment close to 28%.

7.5 Conclusion

As COVID-19 has so vividly demonstrated, pandemics constitute a severe National Security threat. Big Data Analytics technologies can provide a powerful force multiplier in the endeavour of competent authorities and stakeholders to manage the pandemic while minimising the security threats it poses.

As a crisis is unfolding, uncertainty is a crucial element, and the lack of information is a variable that can obstruct the decision-making process. This chapter has discussed the utilisation of a holistic Data Analytics framework for analysing national security aspects in the context of COVID-19. Two real-world cases were considered where authorities' measures to contain the disease via lockdowns resulted in protests and social unrest, namely Michigan and Texas. In both cases, the system proved its ability to provide early warning well in advance of the demonstrations (six and eight days, respectively). It also demonstrated its capacity to provide insights enabling a better understanding and interpretation of the crisis.

Chapter 8

Concluding Remarks

A new methodology to analyse national security based on numerous computational techniques has been introduced in this thesis. These methods have been built upon the idea that a complex problem such as the investigation of national security can be dissected in different components, which work as a powerful tool to create a big picture of a disruptive incident.

Despite the fact that different works have been done to study the aforementioned problem, to the best of my knowledge, none has been focused on extracting numerous insights and joining them to detect a tipping point first and then create a complex methodology concentrated on interpreting a crisis; where this last process plays a critical element since the absence of a timely gaze, an incident can evolve to compromise the stability of a state.

8.1 Contributions

Several key contributions towards examining national security based on machine learning, natural language processing, and other computational techniques have been demonstrated in this work.

In Chapter 3, a conceptual framework for examining social movements has been described. Three main stages (Detonating Event, Warning Period and Crisis Interpretation) help understand and spot pernicious threats by providing valuable insights, which can work as a critical asset for policymakers to determine the best

course of action to tackle an incident.

In Chapter 4, an Alert Mechanism centred on detecting situations where a critical group of individuals feel attracted towards a disruptive ideal has been portrayed. Such a mechanism is supported by the examination of three main elements, namely, Global Polarisation, Social Media Connectedness and Human Security Impact. All of them work in sequence and are grounded on techniques such as sentiment analysis and machine learning classification models. The validity and robustness of this mechanism have been proved in different cases throughout this work.

The following three Chapters describe methodologies linked to the crisis interpretation stage. In connection with this aspect in Chapter 5, Web Insights are dissected, which refers to those multiple web resources embedded in digital messages. The Web Insights investigation is concentrated on comprehending the nature of a crisis. The process starts with the study of the escalation of the crisis over time using machine learning classification models. Then, the main actors' information (Social Networking Services, Information Outlets, Non-Governmental Organisations and Independent Websites) is analysed. Finally, the process estimates whether the studied event has violent-related nuances.

Moreover, in Chapter 6, radical behavioural traits are extracted following two main processes. At first, the identification of instability scenarios based on the Human Security spectrum. Then, the detection and interpretation of behavioural patterns that outline radical demeanour.

Chapter 7 discloses ideological features by using data analytics and machine learning techniques to complement and finalise the crisis interpretation phase. As part of the ideology process, authoritarianism and hostility traits are spotted to unveil national security instabilities.

It should be noted that, in all the three Chapters mentioned above, the validity and robustness were tested by examining numerous actual disruptive events.

As described in previous Chapters, the study of National Security involves different human security components. In line with this aspect, health is one critical element that needs special attention. The core importance of such a fact was evidenced during the pandemic the world dealt with. Hence, consistent with this topic,

Chapter 8 uses the methodologies described in the former chapters to investigate the impact of COVID-19 on National Security stability. For this purpose, two cases were used to validate the whole conceptual framework.

8.2 Limitations

The data corpora used for training and evaluation of this work have limitations. Initially, incidents are triggered by numerous factors suchlike protests, riots or even violent events. However, violence might be resulted due to terrorist circumstances, warfare, societal or political affairs. Then, the narrative and, therefore, the verbs, nouns, and slang expressions suffer variations consequently. All the aspects depicted previously add a tint of complexity because they contribute to bias in the training phase, especially for the alert mechanism, as detecting a tipping point depends on three elements: Global Polarisation, Social Media Connectedness, and Human Security Impact. As described in Chapter 4, Social Media Connectedness refers to the length of time a mass of individuals felt involved and associated with a disruptive cause and considering a nuance of events can create inconsistency in the time-span where people are engaged due to the genesis of the incidents.

Secondly, the nature of events evolves and changes on a daily basis. An example of such an aspect is the pandemic that affected and created havoc worldwide, where new terms and even verbs and slang expressions appeared constantly. As a result of this, the human security components classification can be affected, and the creation of dynamic wordlists is a keystone that must be considered to train new models.

8.3 Future Work

The capability for analysing National Security incidents using the methodology described in Chapters 3 to 7 has been shown by examining various actual events. Nevertheless, different avenues can be explored to improve this work. Firstly, the inclusion of other incidents with various triggering factors can reduce the bias during the training phases. Secondly, supplementary knowledge bases such as Wikipedia

or DBpedia improve/expand the classification of locations and web resources used in the crisis interpretation phase. Thirdly, the proposed methodology requires a dynamic feed of data, which can adapt to actual purposes for policymakers and the decision-making process.

Bibliography

[1] Burch, K.: Parhessia as a principle of democratic pedagogy. Philosophical Studies in Education 40, 71–82 (2009)

[2] Castillo C.: Big Crisis Data: Social Media in Disasters and Time-Critical Situations. Cambridge University Press, (2016).

[3] Zhou, Q., and Jing, M.:Detecting Expressional Anomie in Social Media via Fine-grained Content Mining. Journal of Database Management (JDM), 31(1), 1-19 (2020).

[4] Threat Landscape. https://www.cpni.gov.uk/threat-landscape. Last accesed 14 June 2021.

[5] Annual Threat Assessment of the US Intelligence Community. Office of the Director of National Intelligence, (2021).

[6] A Strong Britain in an Age of Uncertainty: The National Security Strategy. HM Government, (2010).

[7] United Nations Development Program: Human Development Report. New York and Oxford:Oxford University Press, 22-33 (1994).

[8] Institute for Economics and Peace: Global Peace Index 2020. Measuring Peace in a Complex World. (2020).

[9] Keenan, Thomas. The Libyan Uprising and the Right of Revolution in International Law. International and Comparative Law Review.(2011).

[10] Balata, Sundus. The Egyptian Uprising: A Movement in the Making. (2011).

[11] Gregory-River C., Lasalle-Morillo N., Robles L.M., Martinez E., Parrila A., River P. D.M., Rodriguez E., Soto E., Baez V.R.: Temporal Puerto Rican Resistance, Columbia College Chicago. (2019).

[12] Meyer C.O, Bricknell M., Pacheco P. R. and Jones B.: How the COVID-19 crisis has affected security and defence-related aspects of the EU. European Parliament's Subcommittee on Security and Defence, (2021).

[13] Martin, G. Protest, policing and law during COVID-19: On the legality of mass gatherings in a health crisis. Alternative Law Journal, 46(4), 275–281.(2021).

[14] BBC Homepage, `https://www.bbc.co.uk/news/uk-scotland-edinburgh-east-fife-55601318`. Last accessed 21 Mar. 2022.

[15] Stephen L. Cosby: Human Security Concept: The root of U.S. National Security and Foreign Policy. United States Marine Corps,Command and Staff College, Marine Corps Combat Dev,Marine Corps University, South Street,Quantico,VA, 9 (2009).

[16] Axworthy L. : Human Security: Safety for People In a Changing World, Canada Minister of Foreign Affairs, (1999).

[17] Thiago C. J.: Seguridad Nacional, Poder Nacional y Desarrollo. México: CISEN, (1991).

[18] Bennett Moses L., De Koker L., Mendelson D.: Big Data Technology and National Security: Comparative International Perspectives on Strategy, Policy and Law – United Kingdom Report. (2018).

[19] Congressional Research Service: Artificial Intelligence and National Security. (2020).

[20] Mittelsteadt M.: AI Verification, Mechanisms to Ensure AI Arms Control Compliance. Center for Security and Emerging Technology. (2021).

[21] Hurd W. and Kelly R.: Artificial Intelligence and National Security. Center for Security and Emerging Technology and Bipartisan PolicyCenter. (2020).

[22] Babuta A., Oswald M. and Janjeva A.: Artificial Intelligence and UK National Security Policy Considerations. Royal United Services Institute for Defence and Security Studies. (2020).

[23] Dzhekova R., Mancheva M., Stoynova N. and Anagnostou D.: Monitoring Radicalisation A framework for risk indicators. Center for the Study of Democracy, (2017).

[24] The Semantic Analysis against Foreign Fighters Recruitment Online Network Homepage. http://www.saffron-project.eu/en/home/. Last accessed 15 June 2021.

[25] The Detecting and Analysing Terrorist-related online contents and financing activities Homepage. https://cordis.europa.eu/project/id/700367. Last accessed 15 June 2021.

[26] The Partnership against violent radicalisation in the cities Homepage. https://cordis.europa.eu/project/id/740072. Last accessed 15 June 2021.

[27] The Terrorism Prevention via Radicalisation Counter-Narrative Home page. https://trivalent-project.eu/the-project/. Last accessed 15 June 2021.

[28] Dolyle, A., et al. The EMBERS architecture for streaming predictive analytics, IEEE International Conference on Big Data, USA. (2014).

[29] Muthiah S., Butler P., Khandpur R. P., Saraf P., Self N., Rozovskaya A., Zhao L., Cadena J., Lu C.-T., Vullikanti A., Marathe A. , Summers K., Katz G., Doyle A., Arredondo J. , Gupta D. K.,Mares D., and Ramakrishnan N.: EMBERS at 4 years: Experiences operating an open source indicators forecasting system, Proceedings of the 22nd ACM SIGKDD. New York, NY, USA. (2016).

[30] Parang S. and Naren R.: EMBERS AutoGSR: Automated Coding of Civil Unrest Events. Proceedings of the 22nd ACM SIGKDD International Confer-

ence on Knowledge Discovery and Data Mining (KDD '16). Association for Computing Machinery, New York, NY, USA. (2016).

[31] De Leede S.,Haupfleisch R., Korolkova K. and Natter M.:Radicalisation and violent extremism –focus on women:How women become radicalised, and how to empower them to prevent radicalisation. Policy Department for Citizens' Rights and Constitutional Affairs. (2017).

[32] Kudlacek D., Phelps M., Castro T. F.J., Miro L. M., Ehimen E., Purcell S., Görgen T., Hadjimatheou K., Sorell T., Halilovic P. M., Karatrantos T., Lortal G., Rooze M., Young H., Van Hermet D.: Towards a Holistic Understanding of the Prevention of Violent Radicalisation in Europe. European Law Enforcement Research Bulletin. (2018).

[33] Deng, S. and Ning, Y.: A Survey on Societal Event Forecasting with Deep Learning, arXiv e-prints (2021).

[34] Smith E. M. ,Smith J., Legg P., and Francis S.: Predicting the occurrence of world news events using recurrent neural networks and auto-regressive moving average models. In UK Workshop on Computational Intelligence. Springer. (2017).

[35] Halkia M., Ferri S., Papazoglou M., Van Damme M S., and Thomakos D.: Conflict Event Modelling: Research Experiment and Event Data Limitations. In Proceedings of the Workshop on Automated Extraction of Socio-political Events from News 2020. (2020).

[36] Wang X., Hao Chen, Zhoujun Li, and Zhonghua Zhao.: Unrest news amount prediction with context-aware attention lstm. In Pacific Rim International Conference on Artificial Intelligence. Springer. (2018).

[37] Nathan H Parrish, Anna L Buczak, Jared T Zook, James P Howard, Brian J Ellison, and Benjamin D Baugher.: Crystal Cube: Multidisciplinary Approach to Disruptive Events Prediction. In International Conference on Applied Human Factors and Ergonomics. Springer. (2018).

[38] Songgaojun Deng, Huzefa Rangwala, and Yue Ning.: Learning Dynamic Context Graphs for Predicting Social Events. In Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. (2019).

[39] Meng, Lu and Rohini K. Srihari.: Leveraging Heterogeneous Data Sources for Civil Unrest Prediction. (2019).

[40] Songgaojun Deng, Huzefa Rangwala, and Yue Ning.: Dynamic Knowledge Graph Based Multi-Event Forecasting. In Proceedings of the 26th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining.(2020).

[41] Hochreiter S.,Schmidhuber J.: Long Short-Term Memory. Neural Computation. (1997).

[42] Chung J., Gulcehre C., KyungHyun Cho, and Bengio Y.: Empirical evaluation of gated recurrent neural networks on sequence modeling. arXiv preprint arXiv:1412.3555 (2014).

[43] Zhang, Si, Tong, Hanghang, Xu, Jiejun and Maciejewski, Ross: Graph convolutional networks: a comprehensive review. Computational Social Networks.(2019)

[44] Perry, R.: What is a Disaster? New Answers to Old Questions. Xilbris, Corp., 161 (2005).

[45] Twitter. Number of monthly active international Twitter users from 1st quarter 2010 to 1st quarter 2019 (in millions). https://www.statista.com/statistics/274565/monthly-active-international-twitter-users/. Last accesed 14 October 2020.

[46] Sandoval-Almazan R. and Gil-Garcia J. R.: Cyberactivism through Social Media: Twitter, YouTube, and the Mexican Political Movement "I'm Number 132". Hawaii International Conference on System Sciences, 1704-1713 (2013).

[47] Storck M.: The role of social media in political mobilisation: A case study of the January 2011 Egyptian uprising. University of St Andrews, Scotland, 3 (2011/12).

[48] Olson, M.: The Logic of Collective Action, Public Goods and the Theory of Groups. Harvard University Press, 7 (2002).

[49] Boyd D. and Golder S. and Lotan G.: Tweet, Tweet, Retweet: Conversational Aspects of Retweeting on Twitter. Hawaii International Conference on System Sciences, 1-10 (2010).

[50] Stallings R.A. Methods of disaster research. Xlibris Publishing, Bloomington, IN. , 49-55 (2003).

[51] Whiting A. and Williams D. : "Why people use social media: a uses and gratifications approach", Qualitative Market Research. An International Journal, Vol. 16 Issue: 4, 362-369 (2013).

[52] Sutton J.N., Spiro E.,Johnson B.,Fitzhugh S., Greczek M. and Butts C.: Connected Communications: Network Structures of Official Communications in a Technological Disaster. International Conference on Information Systems for Crisis Response and Management, 1-10 (2012).

[53] Sha Y., Jinsong Y. and Guoray C.: Detecting Public Sentiment Over PM2.5 Pollution Hazards through analysis of Chinese Microblog. International Conference on Information Systems for Crisis Response and Management, University Park, Pennsylvania, USA, 722-726 (2014).

[54] Bernd R., Florian U. & Clemens H.: Combining machine-learning topic models and spatiotemporal analysis of social media data for disaster footprint and damage assessment, Cartography and Geographic Information Science, 45:4, 362-376, (2018).

[55] Hagras M., Hassan G. & Farag N.: Towards Natural Disasters Detection from Twitter Using Topic Modelling, European Conference on Electrical Engineering and Computer Science (EECS), 272-279, (2017).

[56] Hashimoto T., Kuboyama T. and Chakraborty B.: Topic extraction from millions of tweets using singular value decomposition and feature selection. Asia-Pacific Signal and Information Processing Association Annual Summit and Conference, 1145-1150, (2015).

[57] Ashcroft M. , Fisher A., Kaati L., Omer E. and Prucha N. : Detecting Jihadist Messages on Twitter. European Intelligence and Security Informatics Conference, 161-164 (2015).

[58] Cohen K., Johansson F., Kaati L. and Mork J.C.: Detecting Linguistic Markers for Radical Violence in Social Media. Terrorism and Political Violence Vol. 246-256, (2014).

[59] Castellanos M., Hsu M., Dayal U., Ghosh R., Dekhil M., Ceja C., Puchi M., and Ruiz P.: Intention insider: discovering people's intentions in the social channel. International Conference on Extending Database Technology. ACM, 614–617, (2012).

[60] Levin, B.: English Verb Classes and Alternations: A Preliminary Investigation. Conversation Analysis, Chicago, IL: The University of Chicago Press (1993).

[61] Socher R., Perelygin A., Wu J.Y., Chuang J., Manning C.D., Ng A.Y., and Potts C.: Recursive deep models for semantic compositionality over a sentiment treebank. In Conference on Empirical Methods in Natural Language Processing, (2013).

[62] Havre S., Hetzler B. and Nowell L.: ThemeRiver: visualizing theme changes over time. IEEE Symposium on Information Visualization 2000, 115-123 (2000).

[63] Plutchik, R.: The Nature of Emotions: Human emotions have deep evolutionary roots, a fact that may explain their complexity and provide tools for clinical practice. American Scientist, 89(4), 344-350, (2001).

[64] Blei D.M., Ng A. Y.,and Jordan M.I.. : Latent Dirichlet Allocation. The Journal of Machine Learning Research, 3:993-1022 (2003).

[65] Grun B. and Hornik K.: Topic Models- An R package for fitting Topic Models. Journal of Statistical Software, 40 (2011).

[66] Local Government Association (2006) Integrated Public Sector Vocabulary. Available at: (http://standards.esd.org.uk). Accessed: 7 December 2017).

[67] Cárdenas P., Theodoropoulos G., Obara B. and Kureshi I.: A Conceptual Framework for Social Movements Analytics for National Security. The International Conference on Computational Science, (2018).

[68] Olteanu A., Vieweg S., and Castillo C.: What to expect when the unexpected happens: Social media communications across crises. In Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work and Social Computing, CSCW , 994–1009, NY, USA, 2015.

[69] Higgins E. and Abigail A.: Engaging the Consumer: The Science and Art of the Value Creation Process. Journal of Consumer Psychology, 19 (2), (2009).

[70] Orehek E., Fishman S., Dechesne M., Doosje B., Kruglanski A., Cole A., Saddler B. and Jackson T.: Need for Closure and the Social Response to Terrorism. Basic and Applied Social Psychology,32: 4, 279 — 290 (2010).

[71] Huo Y. J., Kevin R. and Ludwin E. Molina: Testing and Integrative Model of Respect: Implications for Social Engagement and Well-Being. Personality and Social Psychology Bulletin, 20 (10), (2009).

[72] Bel, van D.T., Smolders, K.C.H.J., IJsselsteijn, W.A., Kort, de Y.A.W.: Social connectedness : concept and measurement. 5th International Conference on Intelligent Environments (2009).

[73] Yardi, S., and Body, D.: Dynamic debates: An analysis of group polarization over time on twitter. Bulletin of Science, Technology and Society 5(30), 2010.

[74] Boyd D. and Golder S. and Lotan G.: Tweet, Tweet, Retweet: Conversational Aspects of Retweeting on Twitter. 2010 43rd Hawaii International Conference on System Sciences, 1-10 (2010).

[75] Bollen J., Mao H. and Zeng X: Twitter mood predicts the stock market. Journal of Computational Science Vol. 2, 1 - 8 (2011).

[76] Asur S., Huberman B.,Szabo G. and Wang C.: Trends in Social Media : Persistence and Decay: arXiv:1102.1402 (2011).

[77] Yunsoo Leeand Suk-Ju Kang: Web Scraping Crawling-based Automatic Data Augmentation for Deep Neural Networks-based Vehicle Classifications. IEEE International Conference on Consumer Electronics, (2019).

[78] R. S. Chaulagain, S. Pandey, S. R. Basnet, and S. Shakya: Cloud Based Web Scraping for Big Data Applications. IEEE International Conference on Smart Cloud, (2017).

[79] D. Kurniawati, D. Triawan: Increased information retrieval capabilities on ecommerce websites using scraping techniques. International Conference n Sustainable Information Engineering and Technology, (2018).

[80] Momin Saniya ParvezKhan Shaista Agah TasneemShivankar Sneha RajendraKalpana R. Bodke: Analysis Of Different Web Data Extraction Techniques. International Conference on Smart City and Emerging Technology, (2018).

[81] Patrick J. Cullen and Erik Reichborn-Kjennerud: MCDC Countering Hybrid Warfare Project:Understanding Hybrid Warfare. Multinational Capability Development Campaign, (2017)

[82] Reed T., Belvin K., Hickman M., Kokolus M., Mendoza F., Phelps A. and Reisler K.: Open Source Indicators Program Handbook. The MITRE Corporation, USA (2017).

[83] BBC Homepage, `https://www.bbc.com/bitesize/guides/zyyvtycrevision/4`. Last accessed 21 Mar. 2019.

[84] Omblegya F. and Kernow T.: Settlements: Hierarchy and Settlement Categories. Cornwall Local Development Framework. (2011).

[85] National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience. Department of Homeland Security, (2013).

[86] Korybko A.: Applicability of Hybrid Warfare to Pakistan: Challenges and Possible Responses. National Defence University-Journal, (2017).

[87] Spiro E., Irvine C., DuBois C., Butts C.: Waiting for a retweet: modeling waiting times in information propagation. NIPS workshop of social networks and social media conference (2012).

[88] Homeland Security Digital Library, `https://www.hsdl.org`. Last accessed 23 March 2019.

[89] Cárdenas P., Theodoropoulos G., Obara B. and Kureshi I.: Defining an alert mechanism for detecting likely threats to National Security. IEEE International Conference on Big Data. USA (2018).

[90] Wayback Machine Homepage, `https://archive.org/help/wayback_api.php`. Last accessed 21 Mar. 2019.

[91] Treverton G.F., Thvedt A., Chen A.R., Lee K. and McCue M.: Addressing Hybrid Threats, Swedish Defence University Center for Asymmetric Threat Studies, (2018).

[92] Treverton G.F.: The Intelligence Challenges of Hybrid Threats Focus on Cyber and Virtual Realm, Swedish Defence University Center for Asymmetric Threat Studies, (2018).

[93] Milo D., Draxler P., Klingova K., Misik M. and Pisko M.: Slovak Republic Hybrid Threats Vulnerability Study, Executive Summary, GLOBSEC, (2018).

[94] Svetoka S.: Social Media as a Tool of Hybrid Warfare, NATO Strategic Communication Center of Excellence, (2016).

[95] Heather J.W. and Llana B.: Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise, RAND Corporation, (2018).

[96] Richterova J.: NATO and Hybrid Threats, Prague Student Summit, Model NATO, (2016).

[97] European External Action Service: EUDefence and Security Spring Series: Tackling new threats, (2019).

[98] Monaghan S., Cullen P. and Wegge N.: MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare, Multinational Capability Development Campaign MCDC (2019).

[99] Correa D., Silva L.A., Mondal M., Benevenuto F., and Gummadi K. P.: The Many Shades of Anonymity: Characterizing Anonymous Social Media Content. In Proceedings of the 9th AAAI International Conference on Weblogs and Social Media (2015).

[100] Mengü Murat and Mengü Seda: Violence and Social Media. Athens Journal of Mass Media and Communications- Volume 1 , Issue 3, 211-228 (2015).

[101] Meloy R., Hoffmann J., Guldimann A., James D.: The Role of Warning Behaviors in Threat Assessment: An Exploration and Suggested Typology . Behavioral Sciences and the Law 30, 256-279 (2012).

[102] Cabinet Office: The National Security Strategy of the United Kingdom, Security in an interdependent world. Available at: (https://assets.publishing.service.gov.uk). Accessed: 3 January 2019.

[103] Ray, L.: Shame and the City – 'Looting', Emotions and Social Structure. The Sociological Review, 62(1), 117–136, (2014).

[104] Derczynski L., Maynard D, Rizzo G.,d , Van Erp M. , Gorrell G., Troncy R. , Petrak J. and Bontcheva K.: Analysis of named entity recognition and linking for tweets. Information Processing and Management, 51(2), 32-49 (2015).

[105] Taylor A.: A tidy data model for natural language processing using cleannlp. The R Journal 9(2):1–20 (2017).

[106] Bhatti, Z., Waqas, A., Ismaili, Imdad Ali, Hakro, Dil Nawaz and Soomro, W.J.: Phonetic based SoundEx and ShapeEx algorithm for Sindhi Spell Checker System, (2014).

[107] House of Lords, House of Commons, Joint Committee on National Security Strategy, National Security Strategy and Strategic Defence and Security Review, UK, (2016).

[108] Grezes, J., and de Gelder, B.: Social perception: understanding other people's intentions and emotions through their actions, Social Cognition: Development, Neuroscience, and Autism, eds T. Striano and V. Reid. (Hoboken, NJ: Wiley-Blackwell), 67–78, (2009).

[109] Cárdenas P., Theodoropoulos G. and Obara B.: Web Insights for National Security: Analysing Participative Online Activity to Interpret Crises, IEEE International Conference on Cognitive Informatics and Cognitive Computing, Italy (2019).

[110] Chollet F. and Allaire J. J.: Deep Learning with R. Manning Publications Co., Greenwich, CT, USA, 1st edition, (2018).

[111] Pennington J., Socher R., and Manning C. D.: GloVe: Global vectors for word representation. In EMNLP, (2014).

[112] Sugathadasa K., Ayesha B., de Silva N., Perera A.S., Jayawardana V., Lakmal D. and Perera M.: Synergistic Union of Word2Vec and Lexicon for Domain Specific Semantic Similarity. arXiv:1706.01967 (2017).

[113] Giugni M. G.: Was It Worth the Effort? The Outcomes and Consequences of Social Movements. Annual Review of Sociology, Vol. 24, (1998).

[114] Van Troost D., Van Stekelenburg J., Klandermans B.: Emotions of Protest, Emotions in Politics. Palgrave Studies in Political Psychology series. Palgrave Macmillan, London (2013)

[115] Faragó L.,Kende A., Krekó P.: Justification of intergroup violence – the role of right-wing authoritarianism and propensity for radical action, Dynamics of Asymmetric Conflict,(2019).

[116] Daskin, E.: Justification of violence by terrorist organisations: Comparing ISIS and PKK. Journal of Intelligence and Terrorism Studies,(2016).

[117] Van Dijk, T. A.: Politics, Ideology, and Discourse. Discourse in Society, (2006).

[118] Siegel, S. M.: The relationship of hostility to authoritarianism. The Journal of Abnormal and Social Psychology, (1956).

[119] Altemeyer, B.: Right-Wing Authoritarianism. Winnipeg, Canada: University of Manitoba Press, (1981).

[120] Dunwoody P.T., Funke F.:The Aggression-Submission-Conventionalism Scale: Testing a New Three Factor Measure of Authoritarianism. Journal of Social and Political Psychology, (2016).

[121] Duckitt, J., Bizumic, B., Krauss, S. W., Heled, E.: A tripartite approach to right-wing authoritarianism: The authoritarianism-conservatism-traditionalism model. Political Psychology, (2010).

[122] Hetherington, M. J., Suhay, E.: Authoritarianism, threat, and Americans' support for the war on terror. American Journal of Political Science, (2011).

[123] Maslow, A. H. Authoritarian character structure. Soc. Psychol., (1943).

[124] Matsumoto D. et al.: The Role of Intergroup Emotions in Political Violence, Current Directions in Psychological Science, (2015).

[125] Rudé G.: Ideology and popular protest, Lawrence and Wishart, (1980).

[126] Sharma E., Saha K., Kiranmai Ernala S., Ghoshal S., and De Choudhury M.: Analyzing Ideological Discourse on Social Media: A Case Study of the Abortion Debate. International Conference of The Computational Social Science Society of the Americas, (2017).

[127] Temporao, M., Vande Kerckhove, C., Van der Linden, C., Dufresne, Y., Hendrickx, J.: Ideological Scaling of Social Media Users: A Dynamic Lexicon Approach. Political Analysis, (2018).

[128] Wojcieszak M.: Don't talk to me: effects of ideologically homogeneous online groups and politically dissimilar offline ties on extremism. New Media and Society, (2010).

[129] Hamelin N., Aznay H., Monette C., Kalpakian J.: Trigger factors of terrorism : social marketing analysis as a tool for security studies - a Moroccan case study. International journal of Euro-Mediterranean studies,(2010).

[130] Masroor, F., Khan, Q. N., Aib, I., and Ali, Z.: Polarization and Ideological Weaving in Twitter Discourse of Politicians. Social Media + Society. (2019).

[131] Jasper, J.M.: The Emotions of Protest: Affective and Reactive Emotions In and Around Social Movements. Sociological Forum 13, (1998).

[132] Martins R., Almeida J.J., Rangel Henriques P., Novais P.: Predicting Performance Problems Through Emotional Analysis. SLATE, (2018).

[133] Cárdenas P., Theodoropoulos G. and Obara B. and I. Kureshi.: Analysing Social Media as a Hybrid Tool to Detect and Interpret likely Radical Behavioural Traits for National Security, IEEE International Conference on Big Data. USA, (2019).

[134] Murtagh, F.: Correspondence Factor Analysis of Big Data Sets: A Case Study of 30 Million Words; and Contrasting Analytics using Apache Solr and Correspondence Analysis in R. ArXiv, abs/1507.01529. (2015).

[135] Saif M. M.: Word Affect Intensities. In Proceedings of the 11th Edition of the Language Resources and Evaluation Conference, (2018).

[136] Park L.A.F., Palaniswami M., Ramamohanarao K.: A Novel Web Text Mining Method Using the Discrete Cosine Transform. Principles of Data Mining and Knowledge Discovery, (2002).

[137] Kingma, D.P., Welling, M.: Auto-encoding variational bayes. In Proceedings of the International Conference on Learning Representations, (2014).

[138] Williams M. L., Burnap P.: Cyberhate on Social Media in the aftermath of Woolwich: A Case Study in Computational Criminology and Big Data, The British Journal of Criminolo1gy, Volume 56, Issue 2, (2016).

[139] Saxton, G.D., Niyirora, J.N., Guo, C., Waters, R.D.: #AdvocatingForChange: The strategic use of hashtags in social media advocacy. Advances in Social Work 16(1), (2015).

[140] Gargan N.:Police National Database. CGI Group Homepage, https://www.cgi-group.co.uk/sites/default/files/files_uk/casestudies/Case_Study_-_PND.pdf. Last accessed 10 Aug. 2020.

[141] Tech UK Homepage, https://www.techuk.org/component/techuksecurity/security/download/2302?file=Breaking_down_barriers_Oct_2014_FINAL.pdf. Last accessed 10 Aug. 2020.

[142] College of Policing Homepage, https://www.app.college.police.uk/app-content/information-management/management-of-police-information/collection-and-recording/. Last accessed 10 Aug. 2020.

[143] BAFA Homepage, https://www.bafa.de/SharedDocs/Downloads/EN/Foreign_Trade/afk_war_weapons_list.pdf?__blob=publicationFile&v=2. Last accessed 9 Aug. 2020.

[144] CNN Homepage, https://edition.cnn.com/2019/07/27/us/puerto-rico-governor-scandal-timeline/index.html. Last accessed 10 Aug. 2020.

[145] New York Times Homepage, https://www.nytimes.com/2019/07/27/us/puerto-rico-protests-timeline.html. Last accessed 10 Aug. 2020.

[146] World Health Org. Homepage, https://bit.ly/2XErwrd. Last accessed 2 Jan. 2021.

[147] Kharroubi S, Saleh F. Are Lockdown Measures Effective Against COVID-19?. Front Public Health. 2020;8:549692. Published 2020 Oct 22. doi:10.3389/fpubh.2020.549692.

[148] Peretti-Watel, P., Seror, V., Cortaredona, S., Launay, O., Raude, J., Verger, P., et al. Attitudes about COVID-19 Lockdown among General Population, France, March 2020. Emerg Infect Dis. 2021;27(1):301-303. https://dx.doi.org/10.3201/eid2701.201377. (2021).

[149] Kureshi,I., Theodoropoulos, G., Magina,E., O'Hare, G., Roche,J., Towards An Info-Symbiotic Framework For Disaster Risk Management, the 19th IEEE/ACM International Symposium on Distributed Simulation and Real Time Applications (DS-RT 2015), Xinhua International Hotel, Chengdu, China, October 14 - 16. (2015).

[150] Toth T., Theodoropoulos G., Boland S., Kureshi I., Ghandar A.: Global Challenge Governance: Time for Big Modelling?, 2019 IEEE 18th International Conference on Cognitive Informatics & Cognitive Computing (ICCI*CC), Milan, Italy, pp. 244-253. (2019).

[151] Roff, H., Uncomfortable Ground Truths: Predictive Analytics and National Security. Brookings National Security Report. (2020).

[152] Akhgar, B., Saathoff, G., Arabnia, H., Hill, R., Staniforth, A., Bayerl, P., Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies. Butterworth-Heinemann, Paperback ISBN: 9780128019672, eBook ISBN: 9780128019733. (2015).

[153] ICEWS Homepage, `https://lmt.co/3owTj8L`. Last accessed 10 Jan. 2021.

[154] Zhang X., Li J., Zhang X., Fu J., and Wang D.: Construction of a Geopolitical Environment Simulation and Prediction Platform Coupling Multi-Source Geopolitical Environmental Factors, Science and Technology Review 36, no, 3. (2018).

[155] Van Puyvelde, D. , Coulthart, S. and Hossain, M. S.: Beyond the buzzword: big data and national security decision-making. International Affairs, 93(6). (2017).

[156] Cárdenas P., Theodoropoulos G., Obara B. and Kureshi I.: Unveiling Ideological Features Through Data Analytics to Construe National Security Instabilities, IEEE International Conference on Big Data. USA. (2020).

[157] Idris M.Y.: Social Instability, Policy Uncertainty, and Financial Risk: Evidence from the Egyptian Exchange and Borse de Tunis, Belfer Center for Science and International Affairs Harvard Kennedy School. (2015).

[158] Davies S.E.: National security and pandemics, United Nations, UN Chronicle. (2013).

[159] Klarevas, L., Clarke, C., COVID-19 Is a Threat to National Security. Let's Start Treating It as Such, Just Security. (2020).

[160] Wilson, J., US lockdown protests may have spread virus widely, cellphone data suggests, The Guardian, 18 May. (2020).

[161] Jeffery, A., Scenes of protests across the country demanding states reopen the economy amid coronavirus pandemic, CNBC. 18 April. (2020).

[162] Hundreds protest COVID-19 orders at Texas Capitol, FOX4News Homepage `https://bit.ly/38IA1rl`. Last accessed 14 Jan. 2021.

[163] Hutchinson, B., Operation Gridlock': Convoy in Michigan's capital protests stay-at-home orders, ABCNews. April 16. (2020).

[164] Saunders B.A., Ngo J.: The Right-Wing Authoritarianism Scale. In: Zeigler-Hill V., Shackelford T. (eds) Encyclopedia of Personality and Individual Differences. Springer, Cham.(2017).

[165] Dunwoody, P., Funke, F.. The Aggression-Submission-Conventionalism Scale: Testing a New Three Factor Measure of Authoritarianism. Journal of Social and Political Psychology, North America. (2016).

[166] Troost D., Emotions of Protest, Emotions in Politics. Palgrave Studies in Political Psychology series. Palgrave Macmillan, London. (2013).

Glossary

Horizontal Escalation When multiple instruments of power are being affected through a synchronised action.. 60

Human Security Protection of the welfare of people, and it is divided into seven components: food security, economic security, health security, environmental security, community security, personal security and political security.. 3

Hybrid Threats They refer to an action conducted by state or non-state actors, whose goal is to undermine or harm a target by combining overt and covert military and non-military means.. 78

Instruments of Power The tools that can be used to assert national power: military, political, economic, civilian and informational.. 60

National Security The defence of territorial integrity, and sovereignty from an external incident.. 3

Radicalisation The process by which a person comes to support terrorism and forms of extremism leading to terrorism.. 10

Vertical Escalation When the intensity of one or many of the instruments of power increases.. 60